

# **MCICOM - Cloudforms**

**July 14, 2014**

**Red Hat, Inc**

**RED HAT Consulting - Confidential**

**Restricted Distribution**

<b>REVISION HISTORY</b>
-------------------------

NUMBER	DATE	DESCRIPTION	NAME
0.1	June 2014	Adding formatting	JS

# Contents

<b>1</b>	<b>Document Information</b>	<b>1</b>
1.1	Originator . . . . .	1
1.2	Owner . . . . .	1
1.3	Copyright . . . . .	1
1.4	Distribution . . . . .	1
1.5	Confidentiality . . . . .	1
1.6	Additional copies . . . . .	1
<b>2</b>	<b>Project Approach</b>	<b>2</b>
2.1	Scope . . . . .	2
2.1.1	Project Scope: . . . . .	2
2.1.2	Proposed Schedule . . . . .	2
2.2	Logistics . . . . .	3
2.3	Contact Information . . . . .	3
<b>3</b>	<b>Cloudforms POC</b>	<b>3</b>
3.1	Architecture . . . . .	3
3.2	Cloudforms Appliance Allocations . . . . .	4
3.2.1	CFME Appliance System Requirements . . . . .	4
3.3	CFME Appliance Setup . . . . .	5
3.3.1	Initial Setup . . . . .	5
3.3.2	Network Configuration . . . . .	5
3.3.3	Hostname Configuration . . . . .	5
3.3.4	Database Configuration . . . . .	5
3.4	Setup POC Cloudformas Appliance Roles . . . . .	6
3.5	Access URL . . . . .	7
3.6	Configure Zones . . . . .	7
3.7	VMware Service Account . . . . .	8
3.8	Install VMware VDDK . . . . .	9
3.9	User Roles . . . . .	9
3.10	Associate Cloudforms Appliance as a VM within vCenter Provider . . . . .	19
3.11	Configure NTP Server . . . . .	20
3.12	Configure outgoing E-mail settings . . . . .	20
3.13	Register Appliance . . . . .	22
3.13.1	Editing Customer Information . . . . .	22

3.14 AD Integration . . . . .	23
3.14.1 Go to the LDAP Configuration Page: . . . . .	23
Configure > Settings > Select EVM Server > Select Authentication Tab . . . . .	23
3.14.2 Fill out the LDAP Settings . . . . .	23
3.15 Add Openstack Provider . . . . .	25
3.16 Add VMware Provider . . . . .	25
3.17 DNS Integration with Infoblox . . . . .	25
3.17.1 Login Information . . . . .	25
3.17.2 Infoblox Access Information . . . . .	26
3.17.3 Infoblox Provisioning Workflow . . . . .	26
3.17.4 Infoblox Retirement Workflow . . . . .	27
3.17.5 Infoblox Automate Overview . . . . .	27
3.17.6 Methods: . . . . .	28
Infoblox_DNS_Alias . . . . .	28
Infoblox_Delete_Record . . . . .	30
Infoblox_Dialog_List_Networks . . . . .	32
Infoblox_Host_Record . . . . .	34
3.18 Import Control Policies, Profiles, Alerts . . . . .	40
3.18.1 Policies.yaml . . . . .	40
3.18.2 Profiles.yaml . . . . .	153
3.18.3 Alerts.yaml . . . . .	251
3.19 Database Backup Procedure . . . . .	267
3.19.1 Web UI: Single Run Database Backup . . . . .	267
3.19.2 Web UI: Scheduled Database Backup . . . . .	267
3.19.3 SSH: Manual Database Backup . . . . .	268
3.20 Member Groups . . . . .	269
3.20.1 Creating/Importing Group from LDAP/Active Directory . . . . .	269
3.20.2 Adding Smart Management Tag to Group . . . . .	270
3.20.3 Groups created during Engagement . . . . .	270
3.21 Tag Taxonomy . . . . .	270
3.21.1 Environment . . . . .	270
3.21.2 Locations . . . . .	271
3.21.3 Owners . . . . .	271
3.21.4 Provisioning Scope . . . . .	271
3.21.5 Storage Types . . . . .	271
3.21.6 Cost Center . . . . .	271
3.21.7 Department . . . . .	272

3.21.8 Workload . . . . .	272
3.21.9 Service Level . . . . .	273
3.21.10 Auto Approve - Max CPU . . . . .	273
3.21.11 Auto Approve - Max Memory . . . . .	273
3.21.12 Auto Approve - Retirement Days . . . . .	273
3.21.13 Auto Approve - Max VM . . . . .	273
3.21.14 Quota - Max Memory . . . . .	274
3.21.15 Quota - Max Storage . . . . .	274
3.21.16 Quota - Max CPU . . . . .	274
3.22 Service Catalog . . . . .	274
3.22.1 Create new Catalogs . . . . .	274
3.22.2 Create New Catalog Item . . . . .	275
3.22.3 Change the Catalog Item Custom Image . . . . .	280
3.22.4 Create New Catalog Bundle . . . . .	281
3.23 Cloudforms: Appendix . . . . .	284
3.23.1 Datastore Import File: infoblox_integration.xml . . . . .	284
<b>4 Issues Encountered</b>	<b>300</b>

# 1 Document Information

## 1.1 Originator

Red Hat Consulting

Jose Simonelli

## 1.2 Owner

Red Hat Consulting – Confidential. Restricted distribution.

## 1.3 Copyright

This document contains proprietary information which is for exclusive use of Red Hat, Inc. and is not to be shared with personnel other than Red Hat, Inc. This document, and any portion thereof, may not be copied, reproduced, photocopied, stored electronically on a retrieval system, or transmitted without the express written consent of the owner.

Red Hat Professional Services does not warrant this document to be free of errors or omissions. Red Hat Professional Services reserves the right to make corrections, updates, revisions, or changes to the information contained herein. Red Hat Professional Services does not warrant the material described herein to be free of patent infringement.

Unless provided otherwise in writing by RED HAT Professional Services, the information and programs described herein are provided “as is” without warranty of any kind, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. In no event will RED HAT Professional Services, its officers, directors, or employees or affiliates of RED HAT Professional Services, their respective officers, directors, or employees be liable to any entity for any special, collateral, incidental, or consequential damages, including without any limitation, for any lost profits or lost savings, related or arising in any way from or out of the use or inability to use the information or programs set forth herein, even if it has been notified of the possibility of such damage by the purchaser or any third party.

## 1.4 Distribution

Do not forward or copy without written permission.

Copies of this document are restricted to the following:

Red Hat, Inc.

MCICOM

## 1.5 Confidentiality

All information supplied to MCICOM for the purpose of this project is to be considered Red Hat confidential.

## 1.6 Additional copies

Further copies of this document can be obtained from:

Jose Simonelli

## 2 Project Approach

### 2.1 Scope

#### 2.1.1 Project Scope:

- [ ] Assist the Customer review and modification of the design and modification of the cloud management implementation, as applicable;
  - [ ] Confirm appliance architecture & sizing
  - [ ] Make adjustments to database cache for optimal performance
  - [ ] General tuning and config (ie. excluding EMS event storm data)
  - [ ] Determine and define database backup strategy
  - [ ] Discuss and define load balancing plan for WebUI's (make appropriate changes to cache settings)
  - [ ] Define and Implement tagging taxonomy
  - [ ] Integrate with Active Directory
  - [ ] Define and configure RBAC
  - [ ] Identify additional point of integration
- [ ] Assist the Customer with the configuration and updates to the current implementation of Red Hat CloudForms per the architectural review as well as the below:
  - [ ] 2 node with HA to serve the dashboard functions
  - [ ] 2 node with HA to serve the snapshot scanning portion
  - [ ] 2 node with HA to handle the provisioning, lifecycle, automation, etc.
- [ ] Assist in the custom design, implementation, and integration of CloudForms with Netapp VSC plugin for enablement of rapid cloning;
  - [ ] Perform the customer implementation to have CloudForms automate and control the Netapp rapid cloning process;
  - [ ] Assist in defining and mentoring on best practices setting up dashboards
- [ ] Assist in the design and setup of Reporting and Dashboards that support the ability to do disk and registry scans/reports;
- [ ] Assist the Customer with the STIG of the CloudForms product

#### 2.1.2 Proposed Schedule

- Duration
  - 6 weeks, Jul 14 – Aug 22
- Start Date
  - July 14, 2014 @ noon
- Travel Schedule
  - Week 1 (7/14 - 7/18)
    - \* On-site support with 2 consultants and 2 DAs
  - Week 2-6 (7/21 - 8/22)
    - \* On-site support with 2 consultants (1 DA available as needed)

## 2.2 Logistics

- Place of Performance
  - 2306 E. Bannister Road, Kansas City, MO 64131-3088
- On-Site Customer Contact
  - Massimo Perreca: 816.394.7588
- Security Requirements
  - JPAS or background check
- Parking
  - [TBD]

## 2.3 Contact Information

Table 1: MCICOM Information

Name	title	Phone	E-mail
Massimo Perreca	Project Manager	816.394.7588	<a href="mailto:Massimo.Perreca.CTR@mcw.ismc.mil">Massimo.Perreca.CTR@mcw.ismc.mil</a>

Table 2: Red Hat Contact Information

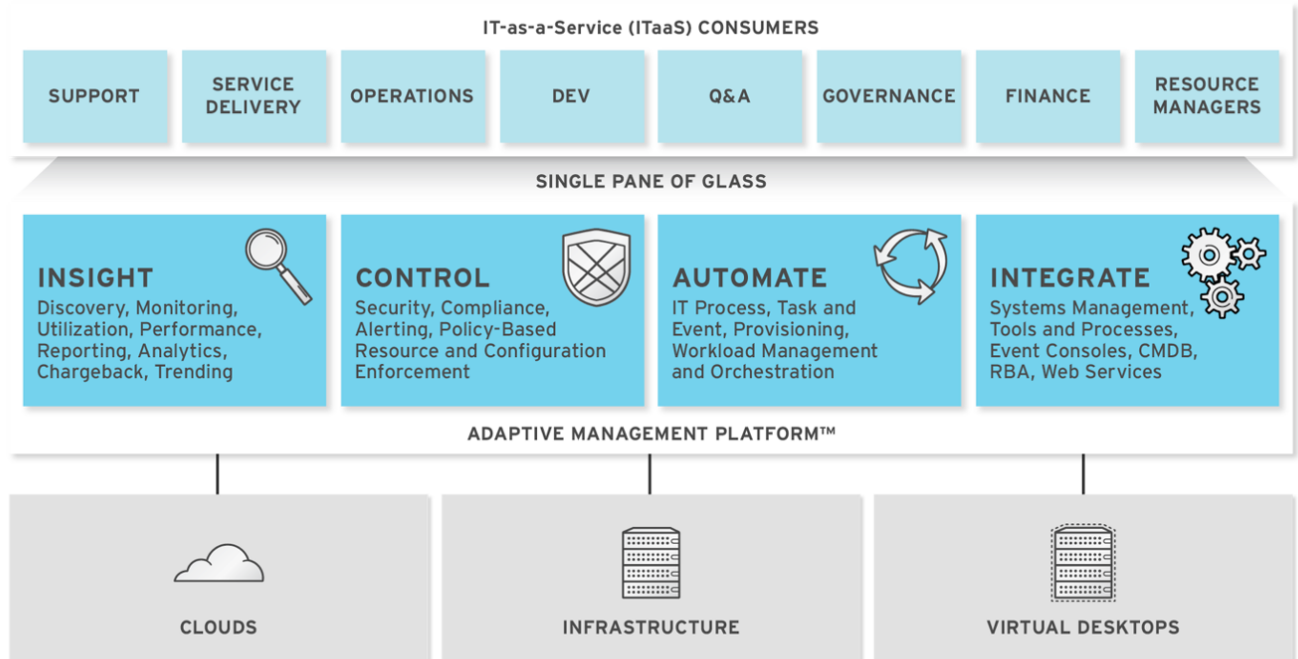
Name	title	Phone	E-mail
Chris Yates	Service Delivery Manager	843-670-2513	<a href="mailto:cyates@redhat.com">cyates@redhat.com</a>
Russ Builta	Domain Architect		<a href="mailto:rbuilt@redhat.com">rbuilt@redhat.com</a>
Jose Simonelli	Domain Architect		<a href="mailto:jose@redhat.com">jose@redhat.com</a>
James Villareal	On-site Consultant		<a href="mailto:jvillarr@redhat.com">jvillarr@redhat.com</a>
Alex Smith	On-Site Consultant		<a href="mailto:alsmith@redhat.com">alsmith@redhat.com</a>

## 3 Cloudforms POC

### 3.1 Architecture

\*The diagram below describes the capabilities of Red Hat CloudForms Management Engine. Its features are designed to work together to provide robust management and maintenance of your virtual infrastructure.





## Features

- The architecture comprises the following components:
  - The CloudForms Management Engine Appliance (Appliance) which is supplied as a secure, high-performance, preconfigured virtual machine. It provides support for Secure Socket Layer (SSL) communications.
  - The CloudForms Management Engine Server (Server) resides on the Appliance. It is the software layer that communicates between the SmartProxy and the Virtual Management Database. It includes support for Secure Socket Layer (SSL) communications.
  - The Virtual Management Database (VMDB) resides either on the Appliance or another computer accessible to the Appliance. It is the definitive source of intelligence collected about your Virtual Infrastructure. It also holds status information regarding Appliance tasks.
  - The CloudForms Management Engine Console (Console) is the Web interface used to view and control the Server and Appliance. It is consumed through Web 2.0 mash-ups and web services (WS Management) interfaces.
  - The SmartProxy can reside on the Appliance or on an ESX Server. If not embedded in the Server, the SmartProxy can be deployed from the Appliance. Each storage location must have a SmartProxy with visibility to it. The SmartProxy acts on behalf of the Appliance communicating with it over HTTPS (SSL) on standard port 443.

### Note

Reference [https://access.redhat.com/documentation/en-US/CloudForms/3.0/html/Management\\_Engine\\_5.2\\_Settings\\_And\\_Operations/-Architecture2.html](https://access.redhat.com/documentation/en-US/CloudForms/3.0/html/Management_Engine_5.2_Settings_And_Operations/-Architecture2.html)

## 3.2 Cloudforms Appliance Allocations

### 3.2.1 CFME Appliance System Requirements

- POC CFME Appliance:

- 1x CFME Appliance:
  - \* 2 vCPU
  - \* 8 GB of RAM
  - \* 1x 40 Root Vol Disk
  - \* 1x 100GB DB Disk
  - \* 1x Network Interface

---

**Note**

[Simplified-CFME-VMDB-Region-Zone-Global-Size-Estimator](#)

---

### 3.3 CFME Appliance Setup

#### 3.3.1 Initial Setup

1. Download the CFME appliance from the Red Hat Customer Portal (login required). The CFME appliance is available as an OVA (Open Virtualization Format) file from: Download Software > Red Hat Enterprise Linux (v. 6 for 64-bit x86\_64) > Red Hat CloudForms Management Engine (v5.2) > VMware Virtual Appliance.
2. Upload the OVA file to the VMware Datastore and create the appliances virtual machines using this file. Convert the virtual machine into a template and use it to create all the appliances.

---

**Note**

To increase performance, increase the default 4 vCPUs/6GB RAM appliance configuration to 4 vCPUs/8GB RAM for the Web UI appliance and 4 vCPUs/8GB RAM for the DB and the Worker appliances.

---

#### 3.3.2 Network Configuration

- Once started, the appliances need to be configured with basic network settings using the virtual serial console in the VMware client. Login as **admin / smartvm** and press Enter to go to the Advanced Settings menu. Set Static Network Configuration, Set Hostname, Set Timezone, Date, and Time. When done entering the settings, select Summary Information to review.
- Host & IP Allocations

Host	IP Address	Netmask	Gateway	DNS Server	Notes
c3pucfme1	10.32.1.228	255.255.254.0	10.32.0.1	10.32.2.53, 10.75.200.141	CFME POC Appliance

#### 3.3.3 Hostname Configuration

- a. Select Option 4
- b. Set the hostname of the CFME appliance. Refer to the table in Network Configuration section

#### 3.3.4 Database Configuration

- With the new appliance the Database is not shipped configured by default. There will need to be a separate Database disk created outside of the appliance and then connected once the appliance has been started. In this case, after looking at where the current

VM count and number of VM's that will be coming over the next few years the Database has been sized to 100GB. This will allow for growth over the next few years.

---

**Note**

The database uses LVM and storage can be extended at a later time

---

- a. On the main console window select Option 10 (To Configure Database)
- b. Select 1) Internal
- c. Select 1) /dev/sdb
- d. Input Region **10** for the Region Selection
- e. Press **Enter**

Region Name	Region #	Notes
Charlotte	10	POC to Production
DBRegion	99	Optional: When Premier decides to scale to have DB Replication

### 3.4 Setup POC Cloudformas Appliance Roles

- Log in to the Cloudforms Web interface and go to Configure > Configuration > Select EVM Appliance > Server Tab
- Check the server roles using the following image as a guide

Server Control

Server Roles

☒ Automation Engine

☒ Capacity & Utilization Coordinator

☒ Capacity & Utilization Data Collector

☒ Capacity & Utilization Data Processor

☒ Database Operations

☐ Database Synchronization

☒ Event Monitor

☒ Notifier

☒ Provider Inventory

☒ Provider Operations

☐ RHN Mirror

☒ Reporting

☒ Scheduler

☒ SmartProxy

☒ SmartState Analysis

☒ User Interface

☒ Web Services

Default Repository SmartProxy

None Available

3.5 Access URL

UI URL
<a href="https://c3pucfme1.premierinc.com">https://c3pucfme1.premierinc.com</a>

3.6 Configure Zones

1. Access the Web Interface and go to Configure > Configuration > Click on Zones
2. In the right frame use the Configuration Icon then select "Add a new zone"

Region Name	Region #	Notes
Charlotte	10	POC to Production
DBRegion	99	Optional: When Premier decides to scale to have DB Replication

### 3.7 VMware Service Account

**Important**

Need a CFME Service Account in order to access VMware vCenter and be able to provision and manage the vCenter environment from Cloudforms

---

**Note**

See the VMware documentation for instructions on how to create a role. This role will need to be associated with whatever credentials you enter for the Management System's instance.

---

- From the Global group, check:
  - Cancel task
  - Diagnostics
  - Log Event
  - Set custom attribute
  - Settings
- The entire set of privileges for the following groups should be checked.
  - Alarms
  - Datastores
  - dvPort Group
  - Host
  - Network
  - Resource
  - Scheduled Task
  - Tasks
  - Virtual Machine
  - vSphere Distributed Switch

In addition, you must also have the following objects and new role in place:

- Datacenter: At the Datacenter the CloudForms Management Engine (CFME) (formerly EVM) user/group must have at least the read-only role at the Datacenter level (Not Propagated) to be able to see the datacenter. Without this access, relationships cannot be made. Specifically, the datastores will not show up.
- Cluster: Each Cluster that the CFME needs access to must have the new role assigned and propagated.
- Folders: Each Folder that CFME needs access to must have the new role assigned and propagated.
- Datastores: Each Datastore that CFME needs access to must have the new role assigned and propagated.
- Networking: Each vLAN or Port Group that CFME needs access to must have the new role assigned and propagated.

---

**Note**

For latest update on this section refer to [Creating Role for CFME in VMware](#) article in Customer Portal

---

### 3.8 Install VMware VDDK

The integration of the VMware VDDK (Virtual Disk Development Kit) optimizes the execution of SmartState Analysis on Virtual Machines and is required for CFME Appliances to successfully collect insight information within VMware vCenter. The VDDK can be downloaded from the VMware website with a valid customer account.

1. Download the VDDK 1.2.2 from VMware's website at <https://my.vmware.com>
2. Download the file VMware-vix-disklib-5.1.1-1042608.x86\_64.tar.gz
3. Copy the file to the /root folder of the CFME Appliances
4. Start an SSH session into the CFME Appliance
5. Run the following commands to extract and install vmware vddk, accept defaults during the installation process:

```
cd /root
tar xvzf VMware-vix-disklib-5.1.1-1042608.x86_64.tar.gz
cd vmware-vix-disklib-distrib
./vmware-install.pl
```

1. Once the VDDK is installed, run the ldconfig command in order for EVM to find the newly installed vddk library.:

```
ldconfig
```

1. Reboot the CloudForms Appliance. The VDDK is now installed on the CFME appliance.

#### Note

Reference: <https://access.redhat.com/knowledge/articles/329683>

### 3.9 User Roles

Access Type	Super Admin	Admin	Developer	Manager
Everything	X			
- Cloud Intelligence	X	X	X	X
.. - Dashboard	X	X	X	X
... - View	X	X	X	X
... - Modify	X	X	X	X
..... - Add and Remove a Widget	X	X	X	X
..... - Reset Dashboard Widgets	X	X	X	X
.. - Reports	X	X		X
... - Dashboard Widgets	X	X		X
..... - Operate	X	X		X
..... - Generate Content	X	X		X
..... - Modify	X	X		X
..... - Add	X	X		X
..... - Copy	X	X		X
..... - Delete	X	X		X
..... - Edit	X	X		X
... - Dashboards	X	X		X

Access Type	Super Admin	Admin	Developer	Manager
..... - Modify	X	X		X
..... - Add	X	X		X
..... - Copy	X	X		X
..... - Delete	X	X		X
..... - Edit	X	X		X
..... - Edit Sequence	X	X		X
... - Edit Report Menus	X	X		
... - Import / Export	X	X		X
... - Reports	X	X		X
..... - View	X	X		X
..... - Operate	X	X		X
..... - Run a selected Report	X	X		X
..... - Modify	X	X		X
..... - Add	X	X		X
..... - Copy	X	X		X
..... - Copy	X	X		X
..... - Delete	X	X		X
..... - Download CSV Format	X	X		X
..... - Download PDF Format	X	X		X
..... - Download Text Format	X	X		X
..... - Edit	X	X		X
... - Saved Reports	X	X		X
..... - Modify	X	X		X
..... - Delete	X	X		X
... - Schedules	X	X		X
..... - Operate	X	X		X
..... - Run Now	X	X		X
..... - Modify	X	X		X
..... - Add	X	X		X
..... - Copy	X	X		X
..... - Delete	X	X		X
..... - Disable	X	X		X
..... - Edit	X	X		X
..... - Enable	X	X		X
.. - Chargeback	X	X		X
... - Assignments	X	X		X
... - Rates	X	X		X
..... - Add	X	X		X
..... - Copy	X	X		X
..... - Copy	X	X		X
..... - Delete	X	X		X
..... - Edit	X	X		X
... - Reports	X	X		X
.. - Timelines	X	X	X	X
.. - RSS	X	X	X	X
- Services	X	X	X	X
.. - My Services	X	X	X	
... - All Services	X	X	X	
..... - View All Services	X	X	X	
..... - Operate	X	X	X	
..... - Edit Tags	X	X		
..... - Retire Services	X	X	X	
..... - Set Retirement Date	X	X	X	

Access Type	Super Admin	Admin	Developer	Manager
..... - Modify	X	X	X	
..... - Set Ownership	X	X		
..... - Edit Services	X	X	X	
..... - Remove Services	X	X	X	
.. - Catalogs Explorer	X	X	X	
... - Catalog Items	X	X		
..... - View Catalog Items	X	X		
..... - Operate	X	X		
..... - Edit Tags	X	X		
..... - Modify	X	X		
..... - Add Atomic Catalog Item	X	X		
..... - Add Composite Catalog Item	X	X		
..... - Edit Atomic Catalog Item	X	X		
..... - Edit Composite Catalog Item	X	X		
..... - Remove Catalog Item	X	X		
... - Catalogs	X	X	X	
..... - View Catalogs	X	X	X	
..... - Modify	X	X		
..... - Add Catalog	X	X		
..... - Edit Catalog	X	X		
..... - Remove Catalog	X	X		
... - Service Catalogs	X	X	X	
..... - Modify	X	X	X	
..... - Provision Services	X	X	X	
.. - Requests	X	X	X	X
... - View	X	X	X	X
..... - List	X	X	X	X
..... - Show	X	X	X	
... - Operate	X	X		X
..... - Approve and Deny	X	X		X
... - Modify	X	X	X	
..... - Copy	X	X	X	
..... - Delete	X	X	X	
..... - Edit	X	X	X	
.. - Workloads	X	X	X	X
... - Accordions	X	X	X	X
..... - Templates & Images	X	X	X	X
..... - VMs & Instances	X	X	X	X
- Clouds	X	X	X	X
.. - Cloud Providers	X	X	X	
... - View	X	X	X	
..... - List	X	X	X	
..... - Show	X	X	X	
..... - Timeline	X	X	X	
... - Operate	X	X		
..... - Discover	X	X		
..... - Edit Tags	X	X		
..... - Manage Policies	X	X		
..... - Refresh	X	X		
... - Modify	X	X		
..... - Add	X	X		



Access Type	Super Admin	Admin	Developer	Manager
..... - Edit	X	X		
..... - Remove	X	X		
.. - Availability Zones	X	X		
... - View	X	X		
..... - List	X	X		
..... - Show	X	X		
..... - Timeline	X	X		
..... - Utilization	X	X		
... - Operate	X	X		
..... - Edit Tags	X	X		
.. - Flavors	X	X		
... - View	X	X		
..... - List	X	X		
..... - Show	X	X		
... - Operate	X	X		
..... - Edit Tags	X	X		
.. - Security Groups	X	X		
... - View	X	X		
..... - List	X	X		
..... - Show	X	X		
... - Operate	X	X		
..... - Edit Tags	X	X		
.. - Instances	X	X	X	X
... - Accordions	X	X	X	
..... - Images	X	X	X	
..... - Images by Provider	X	X	X	
..... - Instances	X	X	X	
..... - Instances by Provider	X	X	X	
... - Image Access Rules	X	X	X	
..... - View	X	X	X	X
..... - Compare	X	X	X	X
..... - Drift	X	X	X	X
..... - List	X	X	X	X
..... - Show	X	X	X	X
..... - Timelines	X	X	X	X
..... - Utilization	X	X	X	X
..... - Operate	X	X		X
..... - Check Compliance	X	X		X
..... - Edit Tags	X	X		X
..... - Manage Policies	X	X		X
..... - Policy Simulation	X	X		X
..... - Refresh	X	X		X
..... - Set Ownership	X	X		X
..... - Modify	X	X		
..... - Edit	X	X		X
..... - Edit EVM Server Relationship	X	X		
..... - Remove	X	X		X
... - Instance Access Rules	X	X	X	
..... - View	X	X	X	X
..... - Compare	X	X	X	X
..... - Drift	X	X	X	X
..... - List	X	X	X	X

Access Type	Super Admin	Admin	Developer	Manager
..... - Show	X	X	X	X
..... - Timelines	X	X	X	X
..... - Utilization	X	X	X	X
..... - Operate	X	X		
..... - Check Compliance	X	X		X
..... - Edit Tags	X	X		X
..... - Manage Policies	X	X		X
..... - Policy Simulation	X	X		X
..... - Power Off	X	X	X	
..... - Power On	X	X	X	
..... - Refresh	X	X	X	
..... - Reset	X	X	X	
..... - Restart Guest	X	X	X	
..... - Retire Instances	X	X	X	X
..... - Set Ownership	X	X		
..... - Set Retirement Date	X	X	X	X
..... - Shutdown Guest	X	X	X	
..... - Suspend	X	X	X	
..... - Terminate	X	X		
..... - Modify	X	X	X	
..... - Edit	X	X		
..... - Edit EVM Server Relationship	X	X		
..... - Provision Instances	X	X	X	
..... - Remove	X	X		
- Infrastructure	X	X	X	X
.. - Infrastructure Providers	X	X		X
... - View	X	X		X
..... - List	X	X		X
..... - Show	X	X		X
..... - Timeline	X	X		X
... - Operate	X	X		
..... - Discover	X	X		
..... - Edit Tags	X	X		X
..... - Manage Policies	X	X		
..... - Refresh	X	X		
... - Modify	X	X		
..... - Add	X	X		
..... - Edit	X	X		
..... - Remove	X	X		
.. - Clusters	X	X		X
... - View	X	X		X
..... - Compare	X	X		X
..... - Drift	X	X		X
..... - List	X	X		X
..... - Show	X	X		X
..... - Timelines	X	X		X
..... - Utilization	X	X		X
... - Operate	X	X		
..... - Analysis	X	X		
..... - Manage Policies	X	X		
..... - Tag	X	X		X
... - Modify	X	X		

Access Type	Super Admin	Admin	Developer	Manager
..... - Remove	X	X		
.. - Hosts	X	X		X
... - View	X	X		X
..... - Compare	X	X		X
..... - Drift	X	X		X
..... - List	X	X		X
..... - Show	X	X		X
..... - Timelines	X	X		X
..... - Utilization	X	X		X
... - Operate	X	X		
..... - Analysis	X	X		X
..... - Analyze then Check Compliance	X	X		X
..... - Check Compliance	X	X		X
..... - Discover	X	X		
..... - Edit Tags	X	X		X
..... - Enter Maintenance Mode	X	X		
..... - Exit Maintenance Mode	X	X		
..... - Manage Policies	X	X		
..... - Power Off	X	X		
..... - Power On	X	X		
..... - Refresh	X	X		
..... - Reset	X	X		
..... - Restart Host	X	X		
..... - Shutdown Host	X	X		
..... - Shutdown Host to Standby	X	X		
... - Modify	X	X		
..... - Add	X	X		
..... - Edit	X	X		
..... - Provision Hosts	X	X		
..... - Remove	X	X		
.. - Resource Pools	X	X		X
... - View	X	X		X
..... - List	X	X		X
..... - Show	X	X		X
... - Operate	X	X		X
..... - Edit Tags	X	X		X
..... - Manage Policies	X	X		
... - Modify	X	X		
..... - Remove	X	X		
.. - Datastores	X	X		X
... - View	X	X		X
..... - List	X	X		X
..... - Show	X	X		X
..... - Utilization	X	X		X
... - Operate	X	X		X
..... - Analysis	X	X		
..... - Edit Tags	X	X		X
... - Modify	X	X		
..... - Remove	X	X		
.. - Repositories	X	X		
... - View	X	X		
..... - List	X	X		

Access Type	Super Admin	Admin	Developer	Manager
..... - Show	X	X		
... - Operate	X	X		
..... - Edit Tags	X	X		
..... - Manage Policies	X	X		
..... - Refresh	X	X		
... - Modify	X	X		
..... - Add	X	X		
..... - Edit	X	X		
..... - Remove	X	X		
.. - Virtual Machines	X	X	X	X
... - Accordions	X	X	X	X
..... - Templates	X	X	X	X
..... - VMs	X	X	X	X
..... - VMs & Templates	X	X	X	X
... - Template Access Rules	X	X	X	X
..... - View	X	X	X	X
..... - Compare	X	X	X	X
..... - Drift	X	X	X	X
..... - List	X	X	X	X
..... - Show	X	X	X	X
..... - Timelines	X	X	X	X
..... - Utilization	X	X	X	X
..... - Operate	X	X		X
..... - Analysis	X	X		X
..... - Check Compliance	X	X		X
..... - Edit Tags	X	X		X
..... - Manage Policies	X	X		X
..... - Policy Simulation	X	X		X
..... - Refresh	X	X		X
..... - Set Ownership	X	X		X
..... - Modify	X	X		X
..... - Clone Templates	X	X		
..... - Edit	X	X		X
..... - Edit EVM Server Relationship	X	X		
..... - Remove	X	X		X
..... - Snapshots	X	X	X	X
..... - View	X	X	X	X
..... - List	X	X	X	X
..... - Operate	X	X	X	
..... - Create new Snapshots	X	X	X	
..... - Delete All Existing Snapshots	X	X		
..... - Delete Snapshots	X	X		
..... - Revert to selected snapshot	X	X	X	
... - VM Access Rules	X	X	X	X
..... - View	X	X	X	X
..... - Compare	X	X	X	X
..... - Drift	X	X	X	X
..... - List	X	X	X	X
..... - Show	X	X	X	X
..... - Timelines	X	X	X	X

Access Type	Super Admin	Admin	Developer	Manager
..... - Utilization	X	X	X	X
..... - Operate	X	X	X	X
..... - Analysis	X	X		X
..... - Check Compliance	X	X		X
..... - Console using MKS	X	X	X	
..... - Console using VMRC	X	X	X	
..... - Console using VNC	X	X	X	
..... - Edit Tags	X	X		X
..... - Extract Running Processes	X	X		
..... - Manage Policies	X	X		X
..... - Policy Simulation	X	X		X
..... - Power Off	X	X	X	
..... - Power On	X	X	X	
..... - Refresh	X	X	X	
..... - Reset	X	X	X	
..... - Restart Guest	X	X	X	
..... - Retire VMs	X	X	X	X
..... - Set Ownership	X	X		X
..... - Set Retirement Date	X	X		X
..... - Shutdown Guest	X	X	X	
..... - Suspend	X	X	X	
..... - Modify	X	X	X	X
..... - Mark as VDI Desktops	X	X		
..... - Clone VMs	X	X		
..... - Edit	X	X		X
..... - Edit EVM Server Relationship	X	X		
..... - Migrate VMs	X	X		
..... - Provision VMs	X	X	X	
..... - Publish VMs to a Template	X	X		
..... - Reconfigure VMs	X	X		
..... - Remove	X	X		X
..... - Right-Size VMs	X	X	X	X
..... - Snapshots	X	X	X	X
..... - View	X	X	X	X
..... - List	X	X	X	X
..... - Operate	X	X	X	
..... - Create new Snapshots	X	X	X	
..... - Delete All Existing Snapshots	X	X		
..... - Delete Snapshots	X	X		
..... - Revert to selected snapshot	X	X	X	
.. - PXE	X	X		X
... - Customization Templates	X	X		X
..... - View	X	X		X
..... - Modify	X	X		X
..... - Add	X	X		
..... - Copy	X	X		
..... - Edit	X	X		
..... - Remove	X	X		

Access Type	Super Admin	Admin	Developer	Manager
... - ISO Datastores	X	X		
..... - View	X	X		
..... - Operate	X	X		
..... - Refresh	X	X		
..... - Modify	X	X		
..... - Add	X	X		
..... - Edit ISO Images	X	X		
..... - Remove	X	X		
... - PXE Servers	X	X		
..... - View	X	X		
..... - Operate	X	X		
..... - Refresh	X	X		
..... - Modify	X	X		
..... - Add	X	X		
..... - Edit	X	X		
..... - Edit PXE Image	X	X		
..... - Edit Windows Image	X	X		
..... - Remove	X	X		
... - System Image Types	X	X		
..... - View	X	X		
..... - Modify	X	X		
..... - Add	X	X		
..... - Edit	X	X		
..... - Remove	X	X		
- Control	X	X		X
.. - Explorer	X	X		X
... - View All Records	X	X		X
... - Actions	X	X		
..... - Modify	X	X		
..... - Add	X	X		
..... - Delete	X	X		
..... - Edit	X	X		
... - Alert Profiles	X	X		
..... - Modify	X	X		
..... - Add	X	X		
..... - Delete	X	X		
..... - Edit	X	X		
... - Alerts	X	X		
..... - Modify	X	X		
..... - Add/Copy	X	X		
..... - Delete	X	X		
..... - Edit	X	X		
... - Conditions	X	X		
..... - Host Conditions	X	X		
..... - Modify	X	X		
..... - Add/Copy	X	X		
..... - Delete	X	X		
..... - Edit	X	X		
..... - VM Conditions	X	X		
..... - Modify	X	X		
..... - Add/Copy	X	X		
..... - Delete	X	X		
..... - Edit	X	X		

Access Type	Super Admin	Admin	Developer	Manager
... - Events	X	X		
... - Policies	X	X		
..... - Compliance	X	X		
..... - Host Compliance Policy	X	X		
..... - Modify	X	X		
..... - Add/Copy	X	X		
..... - Delete	X	X		
..... - Edit	X	X		
..... - VM Compliance Policy	X	X		
..... - Modify	X	X		
..... - Add/Copy	X	X		
..... - Delete	X	X		
..... - Edit	X	X		
..... - Control	X	X		
..... - Host Control Policy	X	X		
..... - Modify	X	X		
..... - Add/Copy	X	X		
..... - Delete	X	X		
..... - Edit	X	X		
..... - VM Control Policy	X	X		
..... - Modify	X	X		
..... - Add/Copy	X	X		
..... - Delete	X	X		
..... - Edit	X	X		
... - Policy Profiles	X	X		
..... - Modify	X	X		
..... - Add	X	X		
..... - Delete	X	X		
..... - Edit	X	X		
.. - Simulation	X	X		X
.. - Import/Export	X	X		
.. - Log	X	X		X
- Automate	X			
.. - Explorer	X			
.. - Simulation	X			
.. - Buttons	X			
.. - Import/Export	X			
.. - Log	X			
- Optimize	X	X		X
.. - Utilization	X	X		X
.. - Planning	X	X		X
.. - Bottlenecks	X	X		
- Settings & Operations	X	X	X	X
.. - My Settings	X	X	X	X
... - Modify	X	X	X	X
..... - Default Filters	X	X		
..... - Default Views	X	X	X	X
..... - Time Profiles	X	X	X	X
..... - Visual	X	X	X	X
.. - Tasks	X	X		X
... - View	X	X		X
..... - All Other Tasks	X	X		
..... - All VM Analysis Tasks	X	X		

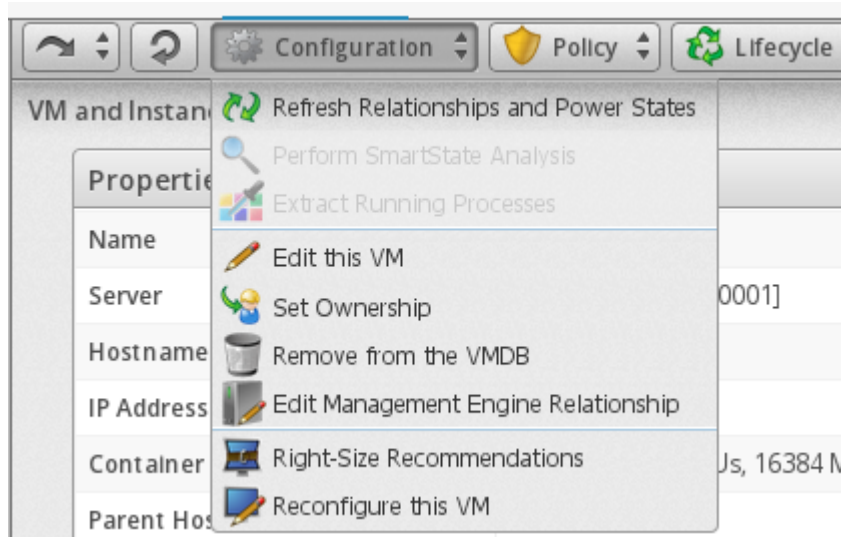
Access Type	Super Admin	Admin	Developer	Manager
.....!- Other UI Tasks	X	X		X
.....!- VM Analysis Tasks	X	X		X
..!- Configuration	X	X		
...!- Access Control	X	X		
...!- Database	X			
...!- Diagnostics	X	X		
...!- Settings	X			
..!- SmartProxies	X	X		
...!- View	X	X		
.....!- List	X	X		
.....!- Show	X	X		
...!- Operate	X	X		
.....!- Deploy	X	X		
...!- Modify	X	X		
.....!- Add	X	X		
.....!- Edit	X	X		
..!- About	X	X	X	X

**Note**

[CFME-rolematrix.xls](#) or [CFME-rolematrix.csv](#)

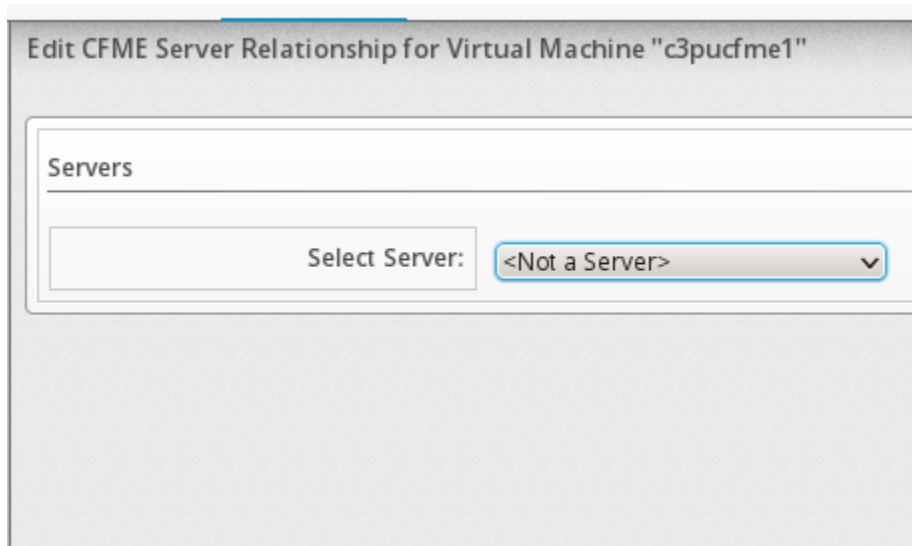
### 3.10 Associate Cloudforms Appliance as a VM within vCenter Provider

In order for Cloudforms to know which appliance is which VM to execute certain jobs it needs to be associated \* Go to Infrastructure > Virtual Machines > Search for <appliance name> (i.e. c3pucfme1) > Click on VM \* In the VM object view Use the VM Configuration menu > Select Edit Management Engine Relationship



- Use the drop down menu to associate the EVM appliance that matches up with this VM. (i.e. EVM10000000000001)





- Click on Save

### 3.11 Configure NTP Server

- Go to Configure > Configuration > Select EVM Server > Click on Server Tab > Enter NTP Information

Label	value
Servers	10.32.198.77

- Click on Save

### 3.12 Configure outgoing E-mail settings

To use the email action in CloudForms Management Engine, you need to set an email address that you will have the emails sent from.


---

**Note**

To be able to send any emails from the server, you must have the Notifier Server role enabled. You can test the settings without the role enabled.

---

### Outgoing SMTP E-mail Server

Host	mailserver.domain.com
Port	25
Domain	domain.com
Start TLS Automatically	<input checked="" type="checkbox"/>
SSL Verify Mode	None
Authentication	login
User Name	admin
Password	
From E-mail Address	admin@domain.com
Test E-mail Address	testemail@domain.com 

- Environment Specific Settings:

Label	value
Host	mailhost.premierinc.com
Port	25
Domain	premierinc.com
Start TLS Automatically	<NOT checked>
SSL Verify Mode	None
Authentication	none
User Name	<blank>
Password	<blank>
From E-mail Address	<a href="mailto:cloudforms@corp.premierinc.com">cloudforms@corp.premierinc.com</a>
Test E-mail Address	

- Use Host to specify the host name of the mail server.
- Use Port to specify the port for the mail server.
- Use Domain to specify domain name for the mail server.
- Check Start TLS Automatically if the mail server requires TLS.

- Select the appropriate SSL Verify Mode.
- Use the Authentication drop down to specify if you want to use login or plain authentication.
- Use User Name to specify the user name required for login authentication.
- Use Password to specify the password for login authentication.
- Use From Email Address to set the address you want to send the email from.
- Use To Email Address if you want to test your email settings.
- Click on Save

### 3.13 Register Appliance

#### 3.13.1 Editing Customer Information

The Red Hat Updates page allows the user to edit customer information.

- To edit customer information
  - Navigate to Configure → Configuration.
  - Click on the Settings accordion, then Region, then click on the Red Hat Updates tab.
  - Click Edit Registration in the Customer Information area
  - The Customer Information area will display options to edit registration, User ID and Password.
    - \* Register to field provides options for the Customer Portal, RHN Satellite v5 for Red Hat Satellite 5.x servers, and RHN Satellite v6 for Red Hat Satellite 6.x servers. If switching to RHN Satellite v5 or v6, the page will refresh and a prompt for a Server URL will be included in the Customer Information area.
    - \* The HTTP Proxy area displays options to enable usage of the HTTP Proxy.
    - \* The User ID and Password are the customer account details for the Customer Portal or Satellite.

---

**Note**

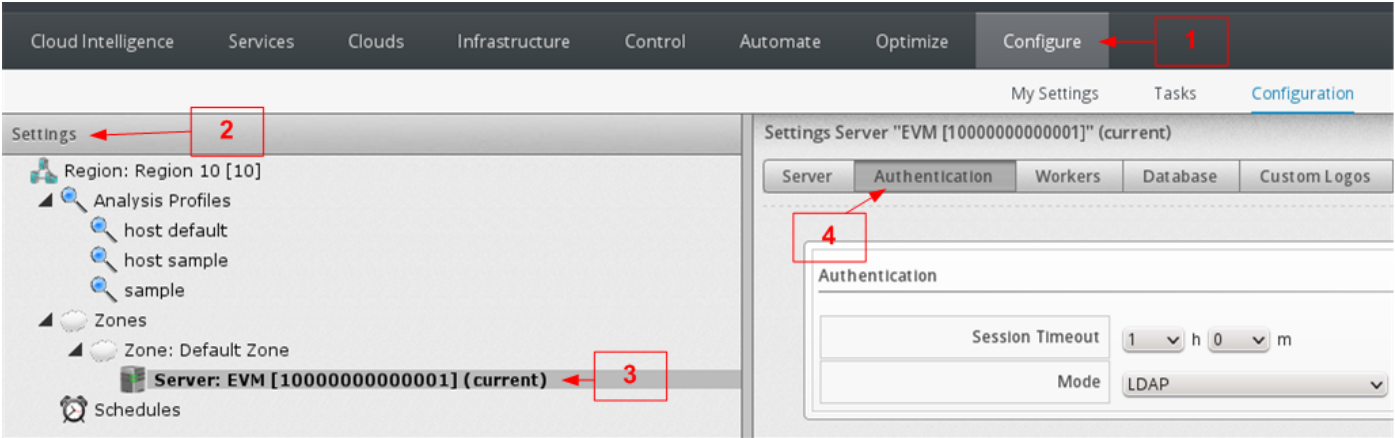
Reference [https://access.redhat.com/documentation/en-US/CloudForms/3.0/html/Management\\_Engine\\_5.2\\_Installation\\_Guide/-chap-Registering\\_and\\_Updating\\_CloudForms\\_Management\\_Engine.html](https://access.redhat.com/documentation/en-US/CloudForms/3.0/html/Management_Engine_5.2_Installation_Guide/-chap-Registering_and_Updating_CloudForms_Management_Engine.html)

---

3.14 AD Integration

3.14.1 Go to the LDAP Configuration Page:

Configure > Settings > Select EVM Server > Select Authentication Tab



3.14.2 Fill out the LDAP Settings

- Set the Session Timeout and Mode

Session Timeout:	[ 1 ]h [ 0 ]m
Mode:	LDAP

Authentication

Session Timeout

1 h 0 m

Mode

LDAP

- Set the LDAP Settings

LDAP Host Names:	c3picorpd5.corp.premierinc.com
LDAP Port:	389
User Type:	E-Mail Address
User Suffix: <user>@	<leave blank>

LDAP Settings

LDAP Host Names

c3picorpd5.corp.premierinc.com

LDAP Port

389

User Type

E-mail Address

User Suffix: <user>@

- Set the Role Settings

Get User Groups from LDAP	<Checked>
Get Roles from Home Forest	<Checked>
Follow Referrals	<Checked>
Base DN:	DC=corp,DC=premierinc,DC=com
Bind DN:	CN=cloudforms,OU=Privileged Accounts,OU=CITS,OU=Corporate Services,DC=corp,DC=premierinc,DC=com
Bind Password:	<See Premier’s Password for this user>

Role Settings

Get User Groups from LDAP

☒

Get Roles from Home Forest

☒

Follow Referrals

☒

Base DN

DC=corp,DC=premierinc,DC=com

Bind DN

CN=cloudforms,OU=Privileged Acco

Bind Password

.....

Validate

- Click [ Validate ]
- Click on Save button at the bottom right of the page

### 3.15 Add Openstack Provider

After initial installation and creation of a CloudForms Management Engine environment, add cloud providers with the following procedure.

- Navigate to Clouds → Providers.
- Click (Configuration), then click (Add a New Cloud Provider).
- Enter a Name for the provider.
- Select the OpenStack in the Provider field
- Fill out the Credentials by typing in a User ID, Password, and a verification of this password (Verify Password).
  - If editing an OpenStack provider, use the AMQP subtab to provide credentials required for the Advanced Message Queuing Protocol service on your OpenStack Nova component.
- Click Validate to validate the credentials.
- Click Add.

### 3.16 Add VMware Provider

After initial installation and creation of a CloudForms Management Engine environment, add providers to the appliance with the following procedure.

- Navigate to Infrastructure → Providers.
- Click (Configuration), then click (Add a New Infrastructure Provider).
- Type in the Name of the provider to add. The Name is how the device is labeled in the console.
- Select the Type of provider: VMware vCenter.
- Type in the Host Name, and IP Address of the provider to add.
- Type in a User ID and Password with administrator privileges to the provider. To refresh a provider, these credentials are required.
- Click Validate to confirm that the user and password connects.
- Click Save.

### 3.17 DNS Integration with Infoblox

#### 3.17.1 Login Information

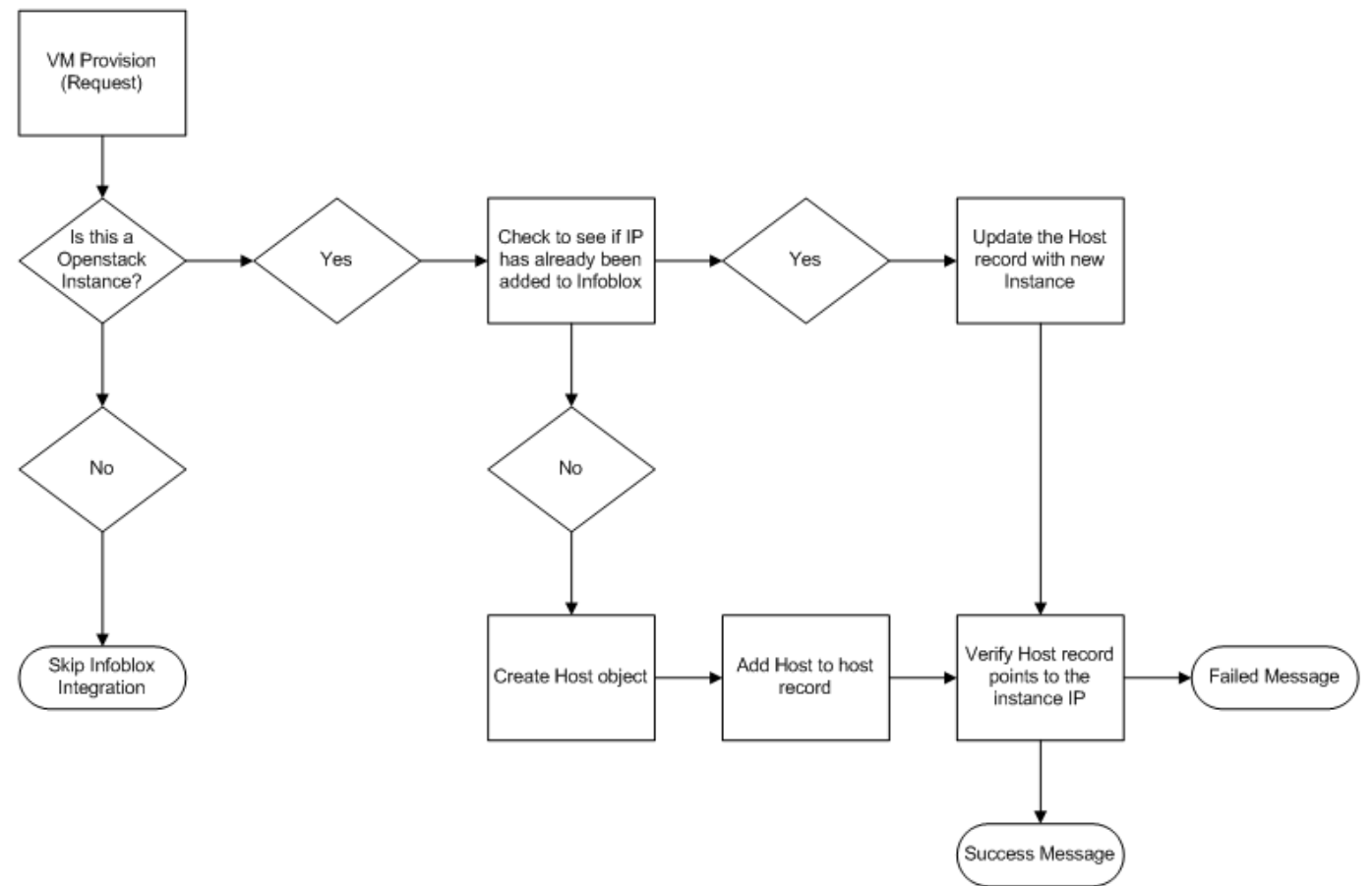
- URL: <https://10.32.2.200/ui/>
- Username: **cloudforms**
- Password: <See Password Sheet with Customer>

3.17.2 Infoblox Access Information

3.17.3 Infoblox Provisioning Workflow

Premier, Inc.  
Cloudforms DNS Integration with Openstack & Infoblox

Provisioning

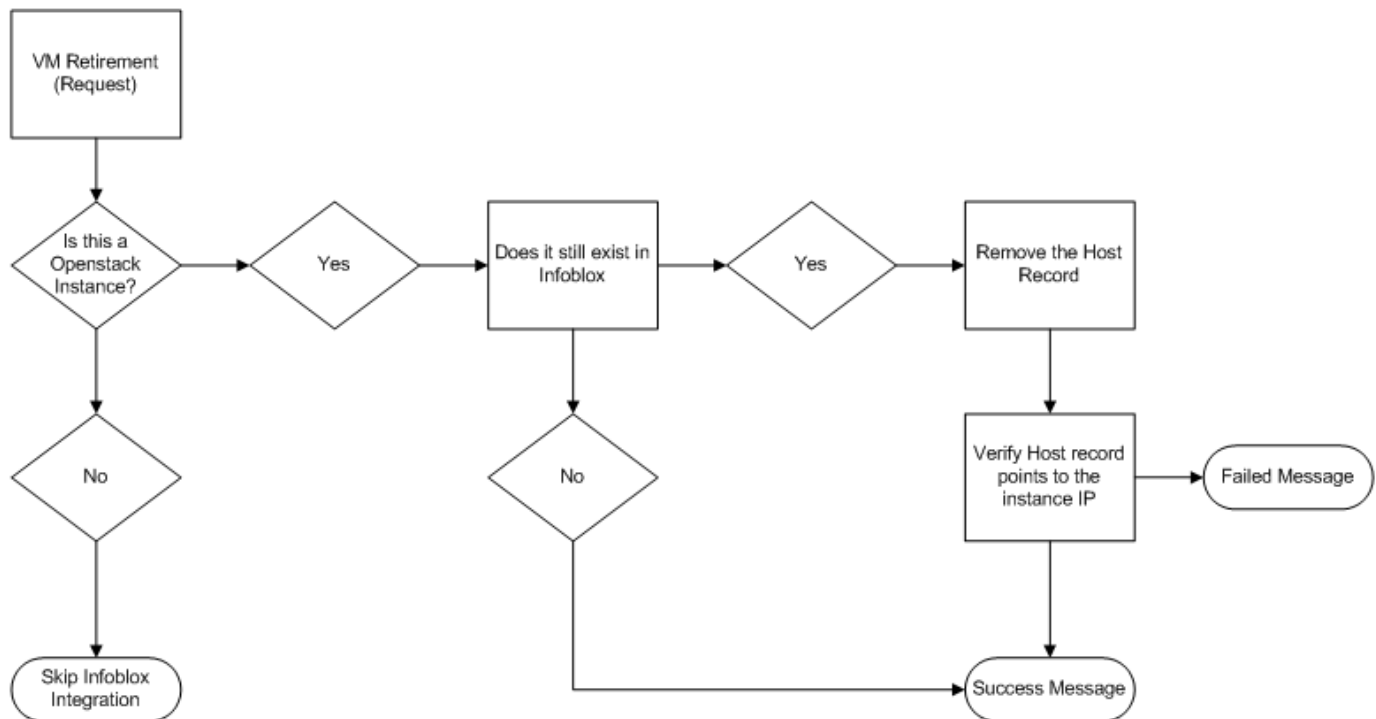


**Note**  
Source: [VSD](#)

### 3.17.4 Infoblox Retirement Workflow

#### Premier, Inc. Cloudforms DNS Integration with Openstack & Infoblox

## Retirement



#### Note

Source: [VSD](#)

### 3.17.5 Infoblox Automate Overview

#### /PremierHealthcare

#### /Integration

##### /Infoblox\_DNS\_Entry

- Instances:
  - Infoblox\_DNS\_Alias
  - Infoblox\_Dialog\_List\_Networks
  - Infoblox\_Host\_Record
  - Infoblox\_Delete\_Record
  - Infoblox\_Instance\_Provision
  - Infoblox\_Instance\_Retire
  - Infoblox\_Instance\_Verify
- Class Schema:



Name	Type	Data Type	Default Value	Display Name	Description	Sub	Collect	Message	On Entry	On Exit	On Error	Collect	Max Retries	Max Time
servername	Attribute	String	infoblox.example.com			[x]		create						
username	Attribute	String	cloudforms			[x]		create						
password	Attribute	Password				[x]		create						
to_email	Attribute	String				[x]		create						
from_email	Attribute	String				[x]		create						
signature	Attribute	String				[x]		create						
action	Attribute	String				[x]		create						
gateway	Attribute	String				[x]		create						
subnet	Attribute	String				[x]		create						
domain	Attribute	String				[x]		create						
method1	Method	String				[x]		create						
method2	Method	String				[x]		create						

### 3.17.6 Methods:

#### Infoblox\_DNS\_Alias

```
#####
#
# EVM Automate Method: Infoblox_DNS_Alias
#
# Notes: EVM Automate method to add Host entry to Infoblox
#
#####
begin
  @method = 'Infoblox_DNS_Alias'
  $evm.log("info", "==== EVM Automate Method: <#{@method}> Started")

  # Turn of verbose logging
  @debug = true

  require 'rest_client'
  require 'json'
  require 'nokogiri'
  require 'ipaddr'

  #####
  # Dump Root Vars
  #####
  def dump_root()
    $evm.log("info", "Root:<$evm.root> Begin $evm.root.attributes")
    $evm.root.attributes.sort.each { |k, v| $evm.log("info", "Root:<$evm.root> Attribute - #{k} ←
      } : #{v}")}
    $evm.log("info", "Root:<$evm.root> End $evm.root.attributes")
    $evm.log("info", "")
  end

  #####
  # Add DNS Alias
  #####
  def addAlias(cname, canonical)
    begin
      url = 'https://' + @connection + '/wapi/v1.0/record:cname'
```

```

    content = "\\{\"name\": \"#{cname}\", \"canonical\": \"#{canonical}\"}"
    dooie = RestClient.post url, content, :content_type => :json, :accept => :json
    $evm.log("info", "==== EVM Automate Method: <#{@method}> Add Alias inspect: #{dooie. ←
      inspect}")
    return true
  rescue Exception => e
    puts e.inspect
    return false
  end
end

#####
# Testing #
#####

# dump all root attributes to the log
dump_root

vm = $evm.root['vm']

username = nil
username ||= $evm.object['username']

password = nil
password ||= $evm.object.decrypt('password')

servername = nil
servername ||= $evm.object['servername']

dnsdomain = nil
dnsdomain ||= $evm.object['domain']

dialog_cname = $evm.root.attributes['dialog_cname'] || nil

@name = "#{vm['name']}.#{dnsdomain}"

@connection = "#{username}:#{password}@#{servername}"

uooie = addAlias("#{dialog_cname}.#{dnsdomain}", "#{@name}")
if uooie == true
  $evm.log("info", "==== EVM Automate Method: <#{@method}> Success: #{dialog_cname}.#{ ←
    dnsdomain} to forward to #{@name}")
else
  $evm.log("info", "==== EVM Automate Method: <#{@method}> FAIL: to add DNS Alias of #{ ←
    dialog_cname}.#{dnsdomain} to forward to #{@name}")
  exit MIQ_ABORT
end

#
# Exit method
#
$evm.log("info", "==== EVM Automate Method: <#{@method}> Ended")
exit MIQ_OK

#
# Set Ruby rescue behavior
#
rescue => err
  $evm.log("error", "<#{@method}>: [{err}]\n#{err.backtrace.join("\n")}")

```

```

exit MIQ_ABORT
end

```

## Infoblox\_Delete\_Record

```

#####
#
# EVM Automate Method: Infoblox_Delete_Record
#
# Notes: EVM Automate method to add Host entry to Infoblox
#
#####
begin
  @method = 'Infoblox_Delete_Record'
  $evm.log("info", "==== EVM Automate Method: <#{@method}> Started")

  # Turn of verbose logging
  @debug = true

  require 'rest_client'
  require 'json'
  require 'nokogiri'
  require 'ipaddr'

  #####
  # Dump Root Vars
  #####
  def dump_root()
    $evm.log("info", "Root:<$evm.root> Begin $evm.root.attributes")
    $evm.root.attributes.sort.each { |k, v| $evm.log("info", "Root:<$evm.root> Attribute - #{k} ←
      ): #{v}") }
    $evm.log("info", "Root:<$evm.root> End $evm.root.attributes")
    $evm.log("info", "")
  end

  #####
  # Fetch Host
  #####
  def fetchHost(host)
    begin
      url = 'https://' + @connection + '/wapi/v1.0/record:host?' + "name=#{host}"
      $evm.log("info", "===== #{url.inspect}")
      dooie = RestClient.get url
      $evm.log("info", "===== #{dooie.inspect}")
      doc = Nokogiri::XML(dooie)
      root = doc.root
      hosts = root.xpath("value/_ref/text()")
      hosts.each do | a |
        a = a.to_s
        unless a.index(host).nil?
          puts "Host Found - #{a}"
          return a
        end
      end
      return true
    rescue Exception => e
      puts e.inspect
    end
  end
end

```

```

        return false
    end
end

#####
# Delete Host                                     #
#####
def deleteHost(item)
    begin
        url = 'https://' + @connection + '/wapi/v1.0/' + item
        dooie = RestClient.delete url
        return true
    rescue Exception => e
        puts e.inspect
        return false
    end
end

#####
# Delete Alias                                     #
#####
def deleteAlias(item)
    begin
        url = 'https://' + @connection + '/wapi/v1.0/' + item
        dooie = RestClient.delete url
        $evm.log("info", "==== EVM Automate Method: <#{@method}> Deleting Alias for host - #{ ↔
            @name} Alias: #{item}")
        return true
    rescue Exception => e
        puts e.inspect
        return false
    end
end

#####
# DeleteAliases                                     #
#####
def findAlias(host)
    begin
        url = 'https://' + @connection + '/wapi/v1.0/record:cname?' + "canonical=#{host}"
        dooie = RestClient.get url
        doc = Nokogiri::XML(dooie)
        root = doc.root
        hosts = root.xpath("value/_ref/text()")
        hosts.each do | a |
            a = a.to_s
            $evm.log("info", "==== EVM Automate Method: <#{@method}> Found Aliases for host - #{ ↔
                @name} Alias: #{a}")
            deleteAlias(a)
        end
        return true
    rescue Exception => e
        puts e.inspect
        return false
    end
end

#####
# Testing                                     #

```

```
#####

# dump all root attributes to the log
dump_root

vm = $evm.root['vm']

username = nil
username ||= $evm.object['username']

password = nil
password ||= $evm.object.decrypt('password')

servername = nil
servername ||= $evm.object['servername']

dnsdomain = nil
dnsdomain ||= $evm.object['domain']

@name = "#{vm['name']}.#{dnsdomain}"

@connection = "#{username}:#{password}@#{@servername}"

$evm.log("info", "==== EVM Automate Method: <#{@method}> Fetching Host: #{@name}")
sooie = fetchHost("#{@name}.#{dnsdomain}")
if sooie == true
  $evm.log("info", "==== EVM Automate Method: <#{@method}> Host: #{@name} does NOT exist")
else
  $evm.log("info", "==== EVM Automate Method: <#{@method}> Fetching Aliases for host - #{ ←
    @name}")
  findAlias(@name)

  $evm.log("info", "==== EVM Automate Method: <#{@method}> Deleting Host - #{sooie}")
  deleteHost(sooie)
end

#
# Exit method
#
$evm.log("info", "==== EVM Automate Method: <#{@method}> Ended")
exit MIQ_OK

#
# Set Ruby rescue behavior
#
rescue => err
  $evm.log("error", "<#{@method}>: [#{err}]\n#{err.backtrace.join("\n")}")
  exit MIQ_ABORT
end
```

### Infoblox\_Dialog\_List\_Networks

```
#####
#
# CFME Automate Method: Infoblox_Dialog_List_Networks
#
```

```

# Author: Kevin Morey
#
# Notes: This method is executed from a Dynamic Drop-down Service Dialog that will list all ↔
#       Infoblox networks and display them in the service dialog
# - gem requirements 'rest_client', 'xmlsimple', 'json'
# dialog_network_cidr
#
#####
begin
  # Method for logging
  def log(level, message)
    @method = 'Infoblox_Dialog_List_Networks'
    $evm.log(level, "#{@method} - #{message}")
  end

  # dump_root
  def dump_root()
    log(:info, "Root:<$evm.root> Begin $evm.root.attributes")
    $evm.root.attributes.sort.each { |k, v| log(:info, "Root:<$evm.root> Attribute - #{k}: #{v} ↔
    }" )
    log(:info, "Root:<$evm.root> End $evm.root.attributes")
    log(:info, "")
  end

  # call_infoblox
  def call_infoblox(action, ref='network' )
    require 'rest_client'
    require 'xmlsimple'
    require 'json'

    servername = nil || $evm.object['servername']
    username = nil || $evm.object['username']
    password = nil || $evm.object.decrypt('password')
    url = "https://#{servername}/wapi/v1.0/"+"#{ref}"

    params = {
      :method=>action,
      :url=>url,
      :user=>username,
      :password=>password,
      :headers=>{ :content_type=>:xml, :accept=>:xml }
    }
    log(:info, "Calling -> Infoblox:<#{url}> action:<#{action}> payload:<#{params[:payload]}>" ↔
    )

    response = RestClient::Request.new(params).execute
    raise "Failure <- Infoblox Response:<#{response.code}>" unless response.code == 200 || ↔
      response.code == 201

    log(:info, "Success <- Infoblox Response:<#{response.code}>")
    # use XmlSimple to convert xml to ruby hash
    response_hash = XmlSimple.xml_in(response)
    log(:info, "Inspecting response_hash: #{response_hash.inspect}")
    return response_hash
  end

  # build_dialog
  def build_dialog(hash)
    dialog_field = $evm.object

```

```

    # set the values to the dialog_hash
    dialog_field['values'] = hash.keys
    # sort_by: value / description / none
    $evm.object["sort_by"] = "description"
    # sort_order: ascending / descending
    $evm.object["sort_order"] = "ascending"
    # data_type: string / integer
    $evm.object["data_type"] = "string"
    # required: true / false
    $evm.object["required"] = "true"

    log(:info, "Dynamic drop down values: #{ $evm.object['values'] }")
    return $evm.object['values']
end

log(:info, "CFME Automate Method Started")

# dump all root attributes to the log
dump_root

# call infoblox to get a list of networks
networks = call_infoblox(:get)

# # only pull out the network and the _ref values
networks_hash = Hash[*networks['value'].collect { |x| [x['network'], x['_ref'][0]] }.flatten <-
]
raise "networks_hash returned nil" if networks_hash.nil?
log(:info, "Inspecting networks_hash:<#{networks_hash}>")

build_dialog(networks_hash)

# Exit method
log(:info, "CFME Automate Method Ended")
exit MIQ_OK

# Set Ruby rescue behavior
rescue => err
  log(:error, "[#{err}]\n#{err.backtrace.join("\n")}")
  exit MIQ_STOP
end

```

## Infoblox\_Host\_Record

```

#####
#
# EVM Automate Method: Infoblox_Host_Record
#
# Notes: EVM Automate method to add Host entry to Infoblox
#
#####
begin
  @method = 'Infoblox_Host_Record'
  $evm.log("info", "==== EVM Automate Method: <#{@method}> Started")

  # Turn of verbose logging
  @debug = true

```

```

require 'rest_client'
require 'json'
require 'nokogiri'
require 'ipaddr'

#####
# Dump Root Vars                                     #
#####
def dump_root()
  $evm.log("info", "Root:<$evm.root> Begin $evm.root.attributes")
  $evm.root.attributes.sort.each { |k, v| $evm.log("info", "Root:<$evm.root> Attribute - #{k} ←
    }: #{v}") }
  $evm.log("info", "Root:<$evm.root> End $evm.root.attributes")
  $evm.log("info", "")
end

#####
# Fetch Host                                           #
#####
def fetchHost(host)
  begin
    url = 'https://' + @connection + '/wapi/v1.0/record:host?' + "name=#{host}"
    $evm.log("info", "===== #{url.inspect}")
    dooie = RestClient.get url
    $evm.log("info", "===== #{dooie.inspect}")
    doc = Nokogiri::XML(dooie)
    root = doc.root
    hosts = root.xpath("value/_ref/text()")
    hosts.each do | a |
      a = a.to_s
      unless a.index(host).nil?
        puts "Host Found - #{a}"
        return a
      end
    end
    return true
  rescue Exception => e
    puts e.inspect
    return false
  end
end

#####
# Delete Host                                           #
#####
def deleteHost(item)
  begin
    url = 'https://' + @connection + '/wapi/v1.0/' + item
    dooie = RestClient.delete url
    return true
  rescue Exception => e
    puts e.inspect
    return false
  end
end

#####
# Get IP Address                                       #

```



```
#####
def getIP(hostname, ipaddress)
  begin
    url = 'https://' + @connection + '/wapi/v1.0/record:host'
    content = "{ \"ipv4addrs\": [ { \"ipv4addr\": \"#{ipaddress}\" } ], \"name\": \"#{hostname} \" } \"}"
    dooie = RestClient.post url, content, :content_type => :json, :accept => :json
    return true
  rescue Exception => e
    puts e.inspect
    return false
  end
end

#####
# Fetch Network Ref #
#####
def fetchNetworkRef(cdir)
  begin
    $evm.log("info", "GetIP --> Network Search - #{cdir}")
    url = 'https://' + @connection + '/wapi/v1.0/network'
    dooie = RestClient.get url
    doc = Nokogiri::XML(dooie)
    root = doc.root
    networks = root.xpath("value/_ref/text()")
    networks.each do | a |
      a = a.to_s
      unless a.index(cdir).nil?
        $evm.log("info", "==== EVM Automate Method: <#{@method}> GetIP --> Network Found - <#{a}>")
        return a
      end
    end
    return nil
  rescue Exception => e
    $evm.log("info", "==== EVM Automate Method: <#{@method}> #{e.inspect}")
    return false
  end
end

#####
# Next Available IP Address #
#####
def nextIP(network)
  begin
    $evm.log("info", "NextIP on - #{network}")
    url = 'https://' + @connection + '/wapi/v1.0/' + network
    dooie = RestClient.post url, :_function => 'next_available_ip', :num => '1'
    doc = Nokogiri::XML(dooie)
    root = doc.root
    nextip = root.xpath("ips/list/value/text()")
    $evm.log("info", "==== EVM Automate Method: <#{@method}> NextIP is - #{nextip}")
    return nextip
  rescue Exception => e
    $evm.log("info", "==== EVM Automate Method: <#{@method}> #{e.inspect}")
    return false
  end
end
end
```

```
#####
#
# Method: validate_ipaddr
# Notes: This method uses a regular expression to validate the ipaddr and gateway
# Returns: Returns string: true/false
#
#####
def validate_ipaddr(ip)
  ip_regex = /\b(?:?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.? \↔
    {3} (?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\b/
  if ip_regex =~ ip
    $evm.log("info", "IP Address:<#{ip}> passed validation") if @debug
    return true
  else
    $evm.log("error", "IP Address:<#{ip}> failed validation") if @debug
    return false
  end
end

#####
# Set Options in prov #
#####
def set_prov(prov, hostname, ipaddr, netmask, gateway)
  $evm.log("info", "GetIP --> Hostname = #{hostname}")
  $evm.log("info", "GetIP --> IP Address = #{ipaddr}")
  $evm.log("info", "GetIP --> Netmask = #{netmask}")
  $evm.log("info", "GetIP --> Gateway = #{gateway}")
  prov.set_option(:sysprep_spec_override, 'true')
  prov.set_option(:addr_mode, ["static", "Static"])
  prov.set_option(:ip_addr, "#{ipaddr}")
  prov.set_option(:subnet_mask, "#{netmask}")
  prov.set_option(:gateway, "#{gateway}")
  prov.set_option(:vm_target_name, "#{hostname}")
  prov.set_option(:linux_host_name, "#{hostname}")
  prov.set_option(:vm_target_hostname, "#{hostname}")
  prov.set_option(:host_name, "#{hostname}")
  $evm.log("info", "GetIP --> #{prov.inspect}")
  $evm.log("info", "GetIP --> #{prov.get_option(:ip_addr)}")

end

#####
# Set netmask #
#####
def netmask(cdir)
  netblock = IPAddr.new(cdir)
  netins = netblock.inspect
  netmask = netins.match(/(?<=\/) (.*) (?=>\/)/)
  $evm.log("info", "GetIP --> Netmask = #{netmask}")
  return netmask
end

#####
# Testing #
#####

# dump all root attributes to the log
dump_root
```

```

action = nil
action ||= $evm.object['action'] || $evm.root['action']
$evm.log("info", "GetIP --> Action= #{action}")

username = nil
username ||= $evm.object['username']

password = nil
password ||= $evm.object.decrypt('password')

servername = nil
servername ||= $evm.object['servername']

subnet = nil
subnet ||= $evm.object['subnet']

gateway = nil
gateway ||= $evm.object['gateway']

dnsdomain = nil
dnsdomain ||= $evm.object['domain']

# Get vm from miq_provision object
prov = $evm.root["miq_provision"]
$evm.log("info", "#{prov.inspect}")

vm_name = prov.options[:vm_target_name]
$evm.log("info", "GetIP --> VM Name = #{vm_name}")

vm_dest_id = prov['destination_id'].to_i
$evm.log("info", "GetIP --> vm_dest_id = #{vm_dest_id.inspect}")

vm_data = $evm.vmdb('vm', vm_dest_id) unless vm_dest_id == 0
$evm.log("info", "GetIP --> vm_data = #{vm_data.inspect}")

ipaddress = vm_data.ipaddresses[0]
$evm.log("info", "GetIP --> IP Address = #{ipaddress}")

@name = "#{vm_name}.#{dnsdomain}"
raise "VM Name was not passed" if @name.empty?

@connection = "#{username}:#{password}@#{servername}"

if vm_data['vendor'] == 'openstack'
  $evm.log("info", "==== EVM Automate Method: <#{@method}> Vendor Type: #{vm_data['vendor'] ←
    '}} Running Infoblox Integration")
  case action

    when "verifyhost"
      $evm.log("info", "==== EVM Automate Method: <#{@method}> Verifying Host: #{@name}.#{ ←
        dnsdomain}")
      sooie = fetchHost("#{@name}.#{dnsdomain}")
      if sooie == true
        $evm.log("info", "==== EVM Automate Method: <#{@method}> Host: #{@name}.#{dnsdomain ←
          } does NOT exist")
      else
        $evm.log("info", "==== EVM Automate Method: <#{@method}> Host: #{@name}.#{dnsdomain ←
          } does exist")
      end
    end
  end
end

```

```

end

when "createhost"
  ipadd = '10.32.18.55'
  $evm.log("info", "==== EVM Automate Method: <#{@method}> IPADD: #{ipadd.inspect} #{ ←
    ipadd.class} -> IPADDRESS #{ipaddress.inspect} #{ipaddress.class}")
  uooie = getIP("#{@name}.#{dnsdomain}", "#{ipaddress}")
  if uooie == true
    $evm.log("info", "==== EVM Automate Method: <#{@method}> #{@name}.#{dnsdomain} with ←
      IP Address #{ipaddress} created successfully")
  elsif uooie == false
    $evm.log("info", "==== EVM Automate Method: <#{@method}> #{@name}.#{dnsdomain} with ←
      IP Address #{ipaddress} FAILED")
    exit MIQ_ABORT
  else
    $evm.log("info", "==== EVM Automate Method: <#{@method}> unknown error")
    exit MIQ_ABORT
  end
end

when "getipnext"
  netRef = fetchNetworkRef(subnet)
  nextIPADDR = nextIP(netRef)
  $evm.log("info", "==== EVM Automate Method: <#{@method}> GetIPNext-before --> #{prov. ←
    options[:vm_target_name]}.#{dnsdomain} with IP Address #{nextIPADDR} created ←
    successfully")
  result = getIP("#{prov.options[:vm_target_name]}.#{dnsdomain}", nextIPADDR)
  $evm.log("info", "==== EVM Automate Method: <#{@method}> GetIPNext-after --> #{prov. ←
    options[:vm_target_name]}.#{dnsdomain} with IP Address #{nextIPADDR} created ←
    successfully")
  if result == true
    $evm.log("info", "==== EVM Automate Method: <#{@method}> GetIP --> #{prov.options[: ←
      vm_target_name]}.#{dnsdomain} with IP Address #{nextIPADDR} created successfully ←
      ")
    netmask = netmask(subnet)
    set_prov(prov, prov.options[:vm_target_name], nextIPADDR, netmask, gateway)
  elsif result == false
    $evm.log("info", "==== EVM Automate Method: <#{@method}> GetIP --> #{prov.options[: ←
      vm_target_name]}.#{dnsdomain} with IP Address #{nextIPADDR} FAILED")
    exit MIQ_ABORT
  else
    $evm.log("info", "==== EVM Automate Method: <#{@method}> GetIP --> unknown error")
  end
end

end
else
  $evm.log("info", "==== EVM Automate Method: <#{@method}> Vendor Type: #{vm_data['vendor ←
    ']} skipping Infoblox Integration")
end

#
# Exit method
#
$evm.log("info", "==== EVM Automate Method: <#{@method}> Ended")
exit MIQ_OK

#
# Set Ruby rescue behavior
#

```

```
rescue => err
  $evm.log("error", "<#{@method}>: [#{err}]\n#{err.backtrace.join("\n")}")
  exit MIQ_ABORT
end
```

### 3.18 Import Control Policies, Profiles, Alerts

- Go to Control > Import/Export
- Click on "Browse" and select the local file to upload
- Click Upload
- Next page will populate showing you all of the items that will be imported
- Click on "Commit"

Do the previous steps for each of the files in the next 3 sections.

#### 3.18.1 Policies.yaml

Link: [Policies.yaml](#)

Source:

```
---
- MiqPolicy:
  name: 427a4378-6519-11df-b637-005056a435be
  description: ! 'Analysis: Post Provisioning'
  expression:
  towhat: Vm
  guid: 427a4378-6519-11df-b637-005056a435be
  created_by: admin
  updated_by: admin
  notes: This policy triggers a vm analysis of any newly provisioned VM
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_provisioned
      description: VM Provision Complete
      guid: 2a17a20a-3e8e-11df-9fe2-005056a435be
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: vm_analyze
      description: Initiate SmartState Analysis for VM
      guid: 5cbel082-ce35-11de-a117-005056b0503e
      action_type: default
      options: {}
    Condition: []
- MiqPolicy:
  name: ! 'Do Not Analyze '
```

```

description: ! 'Analysis: Prevent Analysis of Selected VMs'
expression:
towhat: Vm
guid: 3a7959c0-2866-11de-af2a-0050568026c2
created_by:
updated_by: admin
notes: ! 'This policies prevents analysis ofany vm that is tagged as Do Not Analyze '
active: true
mode: control
MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  failure_synchronous: true
  MiqEvent:
    name: request_vm_scan
    description: VM Analysis Request
    guid: e3292c46-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: prevent
    description: Prevent current event from proceeding
    guid: d885a118-519b-11e0-8d82-005056af0000
    action_type: default
    options: {}
Condition:
- name: Do Not Analyze
  description: VM classified as DO_NOT_ANALYZE
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      CONTAINS:
        tag: Vm.managed-exclusions
        value: do_not_analyze
      context_type:
towhat: Vm
file_mtime:
guid: 39ff4444-08e2-11de-829f-005056a164b2
filename:
applies_to_exp:
miq_policy_id: 10000000000001
notes:
- MiqPolicy:
  name: 782068f8-44ee-11e0-99a6-00505688000a
  description: ! 'Analysis: VDI Login'
  expression:
towhat: Vm
guid: 782068f8-44ee-11e0-99a6-00505688000a
created_by: admin
updated_by: admin
notes: This policy triggers an analysis of a VDI session when a user logs in to
  that session
active: true
mode: control
MiqPolicyContent:
- qualifier: success
  success_sequence: 1

```

```
MiqEvent:
  name: vm_vdi_login_session
  description: VDI Login Session
  guid: 15fc3cce-448a-11e0-9ad1-00505688000a
  event_type: Default
  definition:
  default:
  enabled:
MiqAction:
  name: vm_analyze
  description: Initiate SmartState Analysis for VM
  guid: 5cbel082-ce35-11de-a117-005056b0503e
  action_type: default
  options: {}
Condition: []
- MiqPolicy:
  name: 467f80ce-4808-11df-badc-005056a7121f
  description: ! 'Analysis: VM Configuration Only Profile'
  expression:
  towhat: Vm
  guid: 467f80ce-4808-11df-badc-005056a7121f
  created_by: admin
  updated_by: admin
  notes: ! 'This policy assigns an analysis profile that only gathers vm configuration
    data. Note: the specified action requires that you create an analysis profile
    that only scans vm configuration data. Once it has been created, associate it
    with the specified action'
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_scan_start
      description: VM Analysis Start
      guid: 057b9baa-519c-11e0-8d82-005056af0000
      event_type: Default
      definition:
      default:
      enabled:
    MiqAction:
      name: b52a86f0-4807-11df-badc-005056a7121f
      description: ! 'Profile: VM configuration only'
      guid: b52a86f0-4807-11df-badc-005056a7121f
      action_type: assign_scan_profile
      options:
        :scan_item_set_name: vm configuration only
    Condition: []
- MiqPolicy:
  name: 2f2a1a1c-4806-11df-badc-005056a7121f
  description: ! 'Analysis: VM Reconfiguration'
  expression:
  towhat: Vm
  guid: 2f2a1a1c-4806-11df-badc-005056a7121f
  created_by: admin
  updated_by: admin
  notes: Performs an analysis on any vm that has been reconfigured
  active: true
  mode: control
```

```

MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_reconfigure
    description: VM Settings Change
    guid: 07367e62-449a-11de-bd4f-005056a83e5d
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: vm_analyze
    description: Initiate SmartState Analysis for VM
    guid: 5cbel082-ce35-11de-a117-005056b0503e
    action_type: default
    options: {}
  Condition: []
- MiqPolicy:
  name: d658fe5c-de2c-11e1-9088-005056af009e
  description: Collect Logged on User Info
  expression:
  towhat: Vm
  guid: d658fe5c-de2c-11e1-9088-005056af009e
  created_by: admin
  updated_by: admin
  notes:
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_scan_complete
      description: VM Analysis Complete
      guid: f7b8361e-1139-11e1-9333-005056af009e
      event_type: Default
      definition:
      default:
      enabled:
    MiqAction:
      name: raise_automation_event
      description: Raise Automation Event
      guid: e7da3b7a-1139-11e1-9333-005056af009e
      action_type: default
      options: {}
    Condition:
  - name: ab61c97a-de2e-11e1-9088-005056af009e
    description: Check files starting with nb
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkcount:
            ! '>=':
              value: '1'
              field: <count>
          search:
            INCLUDES:

```



```

        value: nb
        field: Vm.filesystems-name
    context_type:
    towhat: Vm
    file_mtime:
    guid: ab61c97a-de2e-11e1-9088-005056af009e
    filename:
    applies_to_exp:
    miq_policy_id: 5
    notes:
- MiqPolicy:
  name: c66e6d58-d2fc-11de-b4f6-0050568a547d
  description: ! 'Configuration: Host - DMZ Fully Collapsed Advanced Settings'
  expression:
  towhat: Host
  guid: c66e6d58-d2fc-11de-b4f6-0050568a547d
  created_by: admin
  updated_by: admin
  notes: This policy verifies designated host advanced settings values to ensure
    that they meet DMZ requirements
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_scan_complete
      description: Host Analysis Complete
      guid: ffcfb368-455d-11de-86a0-005056a81f62
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: 4fffb6baa-d2e6-11de-b4f6-0050568a547d
      description: Email - DMZ
      guid: 4fffb6baa-d2e6-11de-b4f6-0050568a547d
      action_type: email
      options:
        :variables:
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>

```

```

      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    :to: dmzalert@manageiq.com
Condition:
- name: 1ea32d10-d2fd-11de-b4f6-0050568a547d
  description: host - dmz - advanced settings - ssl
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkall:
          =:
            value: 'true'
            field: Host.advanced_settings-value
        search:
          =:
            value: Config.Defaults.security.host.ruissl
            field: Host.advanced_settings-name
    towhat: Host
    file_mtime:
    guid: 1ea32d10-d2fd-11de-b4f6-0050568a547d
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000013
    notes:
- MiqPolicy:
  name: 8a8f247a-480a-11df-badc-005056a7121f
  description: ! 'Configuration: VM - CPU Reservation > 500Mhz'
  expression:
  towhat: Vm
  guid: 8a8f247a-480a-11df-badc-005056a7121f
  created_by: admin
  updated_by: admin
  notes: Sends an email if CPU reservation is set to a value greater than 500Mhz
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
  MiqEvent:
    name: vm_scan_complete
    description: VM Analysis Complete
    guid: f7b8361e-1139-11e1-9333-005056af009e
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: 5189755e-480a-11df-badc-005056a7121f
    description: Alert - CPU Reservation > 500Mhz

```

```

    guid: 5189755e-480a-11df-badc-005056a7121f
    action_type: evaluate_alerts
    options:
      :alert_guids:
      - ca26a9c6-4802-11df-badc-005056a7121f
    Condition: []
- MiqPolicy:
  name: 6adebf82-d2e4-11de-b4f6-0050568a547d
  description: ! 'Configuration: VM - DMZ Fully Collapsed Network'
  expression:
  towhat: Vm
  guid: 6adebf82-d2e4-11de-b4f6-0050568a547d
  created_by: admin
  updated_by: admin
  notes: ! 'created by: Rod Moore

  purpose: validates vm vlan configuration'
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: vm_reconfigure
    description: VM Settings Change
    guid: 07367e62-449a-11de-bd4f-005056a83e5d
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: 4fffb6baa-d2e6-11de-b4f6-0050568a547d
    description: Email - DMZ
    guid: 4fffb6baa-d2e6-11de-b4f6-0050568a547d
    action_type: email
    options:
      :variables:
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>

```

[illegible]

```

      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    :to: dmzalert@manageiq.com
  - qualifier: failure
    failure_sequence: 2
    MigEvent:
      name: vm_migrate
      description: VM Live Migration (VMOTION)
      guid: 07500602-449a-11de-bd4f-005056a83e5d
      event_type: Default
      definition:
        default:
        enabled:
    MigAction:
      name: vm_shutdown_guest
      description: Shutdown Virtual Machine Guest OS
      guid: 26b84380-bbd5-11de-aaab-0050568a2c6a
      action_type: default
      options: {}
  - qualifier: failure
    failure_sequence: 1
    MigEvent:
      name: assigned_company_tag
      description: Tag Complete
      guid: e384ecb6-1e1e-11de-8918-0050568005db
      event_type: Default
      definition:
        default:
        enabled:
    MigAction:
      name: 4ffb6baa-d2e6-11de-b4f6-0050568a547d
      description: Email - DMZ
      guid: 4ffb6baa-d2e6-11de-b4f6-0050568a547d
      action_type: email
      options:
        :variables:
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>

```

```

      :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
      :to: dmzalert@manageiq.com
  - qualifier: failure
    failure_sequence: 2
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: vm_shutdown_guest
    description: Shutdown Virtual Machine Guest OS
    guid: 26b84380-bbd5-11de-aaab-0050568a2c6a
    action_type: default
    options: {}
  Condition:
  - name: 278843f0-d2e6-11de-b4f6-0050568a547d
    description: vm - vlan - webserver
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        and:
        - FIND:
            checkany:
              IS NOT NULL:
                field: Vm.lans-created_on
            search:
              INCLUDES:
                value: External
                field: Vm.lans-name
        - CONTAINS:
            tag: Vm.managed-function
            value: web_server
  towhat: Vm
  file_mtime:
  guid: 278843f0-d2e6-11de-b4f6-0050568a547d
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000015

```

[illegible]

[illegible]



```

      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      :to: dmzalert@manageiq.com
- qualifier: failure
  failure_sequence: 2
  MiqEvent:
    name: vm_migrate
    description: VM Live Migration (VMOTION)
    guid: 07500602-449a-11de-bd4f-005056a83e5d
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: vm_shutdown_guest
    description: Shutdown Virtual Machine Guest OS
    guid: 26b84380-bbd5-11de-aaab-0050568a2c6a
    action_type: default
    options: {}
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: 4fffb6baa-d2e6-11de-b4f6-0050568a547d
    description: Email - DMZ
    guid: 4fffb6baa-d2e6-11de-b4f6-0050568a547d
    action_type: email
    options:
      :variables:
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>

```

```

      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    :to: dmzalert@manageiq.com
  - qualifier: failure
    failure_sequence: 2
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
        enabled:
  MiqAction:
    name: vm_shutdown_guest
    description: Shutdown Virtual Machine Guest OS
    guid: 26b84380-bbd5-11de-aaab-0050568a2c6a
    action_type: default
    options: {}
  Condition:
  - name: ed4daf4e-d2fa-11de-b4f6-0050568a547d
    description: dmz - windows alerter - disabled
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        =:
          regkey: HKLM\SYSTEM\CurrentControlSet\Services\Alerter
          regval: Start
          value: 4
    towwhat: Vm
    file_mtime:
    guid: ed4daf4e-d2fa-11de-b4f6-0050568a547d
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000016
    notes:
  - name: 469a8766-d2fb-11de-b4f6-0050568a547d
    description: dmz - windows messenger - disabled
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        =:
          regkey: HKLM\SYSTEM\CurrentControlSet\Services\Messenger
          regval: Start
          value: 4
    towwhat: Vm
    file_mtime:
    guid: 469a8766-d2fb-11de-b4f6-0050568a547d
    filename:
    applies_to_exp:

```

```

    miq_policy_id: 10000000000016
    notes:
  - name: 7f648a84-d2fa-11de-b4f6-0050568a547d
    description: dmz - windows automatic update - disabled
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        =:
          regkey: HKLM\SYSTEM\CurrentControlSet\Services\wuauserv
          regval: Start
          value: 4
    towhat: Vm
    file_mtime:
    guid: 7f648a84-d2fa-11de-b4f6-0050568a547d
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000016
    notes:
- MiqPolicy:
  name: de3af0f2-d2f0-11de-b4f6-0050568a547d
  description: ! 'Configuration: VM - Internal Network'
  expression:
  towhat: Vm
  guid: de3af0f2-d2f0-11de-b4f6-0050568a547d
  created_by: admin
  updated_by: admin
  notes: This policy shutdown application or database vms that are incorrectly configured
    to access the dmz network
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: vm_reconfigure
      description: VM Settings Change
      guid: 07367e62-449a-11de-bd4f-005056a83e5d
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: 4ffb6baa-d2e6-11de-b4f6-0050568a547d
      description: Email - DMZ
      guid: 4ffb6baa-d2e6-11de-b4f6-0050568a547d
      action_type: email
      options:
        :variables:
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''

```

```

      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
      :to: dmzalert@manageiq.com
- qualifier: failure
  failure_sequence: 2
  MiqEvent:
    name: vm_reconfigure
    description: VM Settings Change
    guid: 07367e62-449a-11de-bd4f-005056a83e5d
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: vm_shutdown_guest
    description: Shutdown Virtual Machine Guest OS
    guid: 26b84380-bbd5-11de-aaab-0050568a2c6a
    action_type: default
    options: {}
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: vm_migrate
    description: VM Live Migration (VMOTION)
    guid: 07500602-449a-11de-bd4f-005056a83e5d
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: 4ffb6baa-d2e6-11de-b4f6-0050568a547d
    description: Email - DMZ
    guid: 4ffb6baa-d2e6-11de-b4f6-0050568a547d
    action_type: email
    options:
      :variables:
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>

```

[illegible]

```
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
      :to: dmzalert@manageiq.com
- qualifier: failure
  failure_sequence: 2
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1ele-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
        enabled:
          MiqAction:
            name: vm_shutdown_guest
            description: Shutdown Virtual Machine Guest OS
            guid: 26b84380-bbd5-11de-aaab-0050568a2c6a
            action_type: default
            options: {}
  Condition:
    - name: 020dd9c2-d2f1-11de-b4f6-0050568a547d
      description: vm - internal vlan check
      modifier: allow
      expression: !ruby/object:MiqExpression
        exp:
          and:
            - FIND:
                checkany:
                  IS NOT NULL:
                    field: Vm.lans-created_on
                  search:
                    INCLUDES:
```

```

        value: Internal
        field: Vm.lans-name
      - or:
        - CONTAINS:
            tag: Vm.managed-function
            value: application_servers
        - CONTAINS:
            tag: Vm.managed-function
            value: database
    towhat: Vm
    file_mtime:
    guid: 020dd9c2-d2f1-11de-b4f6-0050568a547d
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000014
    notes:
- MiqPolicy:
  name: 56c4d50e-3069-11de-971a-005056a12545
  description: DISA ESX Server STIG - ESX1170 requires IAO/SA to remove or disable
    all unused hardware on VM
  expression:
  towhat: Vm
  guid: 56c4d50e-3069-11de-971a-005056a12545
  created_by:
  updated_by:
  notes:
  active: true
  mode: control
  MiqPolicyContent: []
  Condition:
  - name: 627379ac-3067-11de-971a-005056a12545
    description: ! 'ESX1170: CAT II - Guest OS remove all unused hardware'
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        and:
        - FIND:
            checkcount:
              =:
                value: 0
                field: <count>
            search:
              INCLUDES:
                value: floppy
                field: Vm.hardware.disks-device_type
        - FIND:
            checkcount:
              =:
                value: 0
                field: <count>
            search:
              INCLUDES:
                value: cdrom
                field: Vm.hardware.disks-device_type
    towhat: Vm
    file_mtime:
    guid: 627379ac-3067-11de-971a-005056a12545
    filename:
    applies_to_exp:

```

```

    miq_policy_id: 10000000000010
    notes:
- MiqPolicy:
  name: 69b1559e-3068-11de-971a-005056a12545
  description: DISA ESX Server STIG requires that the Virtual Machine Administrator
    be responsible for the following
  expression:
  towhat: Vm
  guid: 69b1559e-3068-11de-971a-005056a12545
  created_by:
  updated_by:
  notes:
  active: true
  mode: control
  MiqPolicyContent: []
  Condition:
- name: ed826874-3066-11de-971a-005056a12545
  description: ! 'ESX1030: CAT II - Test and Development VMs must be seperated
    from Production VMs'
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      and:
      - FIND:
          checkcount:
            ! '>=':
              value: 1
              field: <count>
          search:
            STARTS WITH:
              value: '192.168'
              field: Vm.hardware.networks-ipaddress
      - CONTAINS:
          tag: Vm.managed-environment
          value: prod
    towhat: Vm
    file_mtime:
    guid: ed826874-3066-11de-971a-005056a12545
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000011
    notes:
- name: 28e35e32-3067-11de-971a-005056a12545
  description: ! 'ESX0940: CAT II - prevent use of nonpersistent disk mode'
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkcount:
          =:
            value: 0
            field: <count>
        search:
          INCLUDES:
            value: nonpersistent
            field: Vm.hardware.disks-mode
    towhat: Vm
    file_mtime:
    guid: 28e35e32-3067-11de-971a-005056a12545

```



```

    filename:
    applies_to_exp:
    miq_policy_id: 10000000000011
    notes:
- MiqPolicy:
  name: de9aa7ec-3069-11de-971a-005056a12545
  description: DISA Information Assurance Vulnerability Alert - MS08-67
  expression:
  towhat: Vm
  guid: de9aa7ec-3069-11de-971a-005056a12545
  created_by:
  updated_by:
  notes:
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: vm_start
      description: VM Power On
      guid: 404b4630-21a8-11e2-b47a-0050568b19a3
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: vm_stop
      description: Stop Virtual Machine
      guid: 37f2da3e-21a8-11e2-b47a-0050568b19a3
      action_type: default
      options: {}
  Condition:
  - name: 7e492e4c-3067-11de-971a-005056a12545
    description: IAVA - MS08-067 for Windows 2000 Service Pack 4
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        and:
        - FIND:
            checkall:
            STARTS WITH:
              value: 5.00.2195.7203
              field: Vm.filesystems-file_version
            search:
              =:
                value: c:/winnt/system32/netapi32.dll
                field: Vm.filesystems-name
        - KEY EXISTS:
            regkey: HKLM\SOFTWARE\Microsoft\Updates\Windows 2000\SP5\KB958644\Filelist
    towhat: Vm
    file_mtime:
    guid: 7e492e4c-3067-11de-971a-005056a12545
    filename:
    applies_to_exp: !ruby/object:MiqExpression
      exp:
        and:
        - STARTS WITH:
            value: Microsoft Windows 2000

```

```

      field: Vm.operating_system-product_name
    - =:
      value: Service Pack 4
      field: Vm.operating_system-service_pack
    miq_policy_id: 10000000000012
    notes:
  - name: 8b0d83d0-3067-11de-971a-005056a12545
    description: IAVA - MS08-067 for Windows Server 2003 Service Pack 1 & 2
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        or:
        - and:
          - =:
            value: Service Pack 1
            field: Vm.operating_system-service_pack
        - FIND:
          checkall:
            STARTS WITH:
              value: 5.2.3790.3229
              field: Vm.filesystems-file_version
          search:
            =:
              value: c:/windows/system32/netapi32.dll
              field: Vm.filesystems-name
        - and:
          - =:
            value: Service Pack 2
            field: Vm.operating_system-service_pack
        - FIND:
          checkall:
            STARTS WITH:
              value: 5.2.3790.4392
              field: Vm.filesystems-file_version
          search:
            =:
              value: c:/windows/system32/netapi32.dll
              field: Vm.filesystems-name
    towhat: Vm
    file_mtime:
    guid: 8b0d83d0-3067-11de-971a-005056a12545
    filename:
    applies_to_exp: !ruby/object:MiqExpression
      exp:
        and:
        - STARTS WITH:
          value: Microsoft Windows Server 2003
          field: Vm.operating_system-product_name
        - or:
          - =:
            value: Service Pack 1
            field: Vm.operating_system-service_pack
          - =:
            value: Service Pack 2
            field: Vm.operating_system-service_pack
    miq_policy_id: 10000000000012
    notes:
  - name: 9482beb2-3067-11de-971a-005056a12545
    description: IAVA - MS08-067 for Windows XP Service Pack 2 & 3

```

```

modifier: allow
expression: !ruby/object:MiqExpression
  exp:
    and:
      - FIND:
          checkall:
            STARTS WITH:
              value: 5.1.2600.3462
              field: Vm.filesystems-file_version
          search:
            =:
              value: c:/windows/system32/netapi32.dll
              field: Vm.filesystems-name
      - KEY EXISTS:
          regkey: HKLM\SOFTWARE\Microsoft\Updates\Windows XP\SP4\KB958644\Filelist
towhat: Vm
file_mtime:
guid: 9482beb2-3067-11de-971a-005056a12545
filename:
applies_to_exp: !ruby/object:MiqExpression
  exp:
    and:
      - STARTS WITH:
          value: Microsoft Windows XP
          field: Vm.operating_system-product_name
      - or:
          - =:
              value: Service Pack 2
              field: Vm.operating_system-service_pack
          - =:
              value: Service Pack 3
              field: Vm.operating_system-service_pack
miq_policy_id: 10000000000012
notes:
- MiqPolicy:
  name: 69fbd202-8ba3-11e0-b8fc-005056a40e59
  description: DMZ - Shutdown VM after Analysis if it has more than 1 NIC
  expression: !ruby/object:MiqExpression
    exp:
      =:
        value: 'on'
        field: Vm-power_state
    context_type:
towhat: Vm
guid: 69fbd202-8ba3-11e0-b8fc-005056a40e59
created_by: admin
updated_by: admin
notes:
active: true
mode: control
MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_scan_complete
    description: VM Analysis Complete
    guid: f7b8361e-1139-11e1-9333-005056af009e
    event_type: Default
    definition:

```

```

    default:
    enabled:
  MiqAction:
    name: vm_shutdown_guest
    description: Shutdown Virtual Machine Guest OS
    guid: 26b84380-bbd5-11de-aaab-0050568a2c6a
    action_type: default
    options: {}
- qualifier: success
  success_sequence: 2
  MiqEvent:
    name: vm_scan_complete
    description: VM Analysis Complete
    guid: f7b8361e-1139-11e1-9333-005056af009e
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: evm_event
    description: Show EVM Event on Timeline
    guid: 16b1810c-44e8-11e0-acda-005056a40e59
    action_type: default
    options: {}
Condition:
- name: efcf3702-8b9e-11e0-b8fc-005056a40e59
  description: DMZ - VM has more than 1 NIC
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      ! '>':
        count: Vm.hardware.nics
        value: '1'
      context_type:
    towhat: Vm
    file_mtime:
    guid: efcf3702-8b9e-11e0-b8fc-005056a40e59
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000077
    notes:
- MiqPolicy:
  name: 0de66508-8b9f-11e0-b8fc-005056a40e59
  description: DMZ - Shutdown VM after Starting if it has more than 1 NIC
  expression:
  towhat: Vm
  guid: 0de66508-8b9f-11e0-b8fc-005056a40e59
  created_by: admin
  updated_by: admin
  notes:
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_start
      description: VM Power On
      guid: 404b4630-21a8-11e2-b47a-0050568b19a3

```

```

    event_type: Default
    definition:
      default:
      enabled:
    MiqAction:
      name: vm_stop
      description: Stop Virtual Machine
      guid: 37f2da3e-21a8-11e2-b47a-0050568b19a3
      action_type: default
      options: {}
- qualifier: success
  success_sequence: 2
  MiqEvent:
    name: vm_start
    description: VM Power On
    guid: 404b4630-21a8-11e2-b47a-0050568b19a3
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: evm_event
    description: Show EVM Event on Timeline
    guid: 16b1810c-44e8-11e0-acda-005056a40e59
    action_type: default
    options: {}
- qualifier: success
  success_sequence: 3
  MiqEvent:
    name: vm_start
    description: VM Power On
    guid: 404b4630-21a8-11e2-b47a-0050568b19a3
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: d91bbabc-b0be-11e1-b0dc-005056b057a8
    description: ! 'VM Attribute: Allowed NIC Count Exceeded'
    guid: d91bbabc-b0be-11e1-b0dc-005056b057a8
    action_type: set_custom_attribute
    options:
      :attribute: EVM Policy
      :value: Allowed NIC Limit Exceeded
  Condition:
- name: efcf3702-8b9e-11e0-b8fc-005056a40e59
  description: DMZ - VM has more than 1 NIC
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      ! '>':
        count: Vm.hardware.nics
        value: '1'
    context_type:
  towhat: Vm
  file_mtime:
  guid: efcf3702-8b9e-11e0-b8fc-005056a40e59
  filename:
  applies_to_exp:

```

```

    miq_policy_id: 10000000000077
    notes:
- MiqPolicy:
  name: 0f2cc826-fa4b-11de-83ca-005056ba0614
  description: Directory Service Used for Authentication for sudo
  expression:
  towhat: Host
  guid: 0f2cc826-fa4b-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that sudo is configured to use a directory for user
    authentication.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
  - name: 684b2a60-fa4b-11de-83ca-005056ba0614
    description: Directory Service used for sudo authentication
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:
              value: ^\s*auth\s+required\s+.*pam_stack\.so\s+service=system-auth
              field: Host.filesystems-contents
            search:
              =:
                value: /etc/pam.d/sudo
                field: Host.filesystems-name
          towhat: Host
          file_mtime:
          guid: 684b2a60-fa4b-11de-83ca-005056ba0614
          filename:
          applies_to_exp:
          miq_policy_id: 10000000000053
          notes: ! 'This condition verifies that the line "auth required pam_stack.so
            service=system-auth" exists in /etc/pam.d/sudo. '
- MiqPolicy:
  name: 1c4c7772-a7fb-11e0-abed-005056af0000
  description: Do Not Analyze Active VDI VMs
  expression:
  towhat: Vm

```

```

guid: 1c4c7772-a7fb-11e0-abed-005056af0000
created_by: admin
updated_by: admin
notes: This policy prevents analysis of a vm that has an active user session
active: true
mode: control
MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_scan_start
    description: VM Analysis Start
    guid: 057b9baa-519c-11e0-8d82-005056af0000
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: prevent
    description: Prevent current event from proceeding
    guid: d885a118-519b-11e0-8d82-005056af0000
    action_type: default
    options: {}
Condition:
- name: 0a50f750-a7fb-11e0-abed-005056af0000
  description: VM has an active session
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      =:
        value: 'true'
        field: Vm-has_active_vdi_session
    context_type:
  towhat: Vm
  file_mtime:
  guid: 0a50f750-a7fb-11e0-abed-005056af0000
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000007
  notes:
- MiqPolicy:
  name: af2d74ea-fa39-11de-83ca-005056ba0614
  description: Firewall - Incoming Security Level
  expression:
  towhat: Host
  guid: af2d74ea-fa39-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that only a defined set of incoming TCP and UDP Ports
    are open.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7

```

```

    event_type: Default
    definition:
      default:
      enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
    Condition:
  - name: b4a0843a-fa43-11de-83ca-005056ba0614
    description: Valid Incoming UDP Ports
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        LIMITED TO:
          value: '427'
          field: Host-enabled_udp_inbound_ports
    towhat: Host
    file_mtime:
    guid: b4a0843a-fa43-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000021
    notes: This condition verifies that the only open incoming UDP port is 427.
  - name: 03529e9e-f961-11de-9e9d-0050568a07c7
    description: Valid Incoming TCP Ports
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        LIMITED TO:
          value: '902,80,443,427,5989,22,5988'
          field: Host-enabled_tcp_inbound_ports
    towhat: Host
    file_mtime:
    guid: 03529e9e-f961-11de-9e9d-0050568a07c7
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000021
    notes: This condition verifies that the only open incoming TCP ports are ←
           22,80,427,443,902,5988,and
           5989.
  - MiqPolicy:
      name: edaf1082-fa54-11de-83ca-005056ba0614
      description: Firewall - Outgoing NTP Port
      expression:
      towhat: Host
      guid: edaf1082-fa54-11de-83ca-005056ba0614
      created_by: admin
      updated_by: admin
      notes: This policy validates that the Firewall is configured properly for NTP
            support.
      active: true
      mode: compliance
      MiqPolicyContent:
        - qualifier: failure
          failure_sequence: 1
      MiqEvent:

```



```

    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
MiqAction:
  name: compliance_failed
  description: Mark as Non-Compliant
  guid: ba452d94-f586-11de-8ebc-0050568a07c7
  action_type: default
  options: {}
Condition:
- name: 1cb7f0ba-fa55-11de-83ca-005056ba0614
  description: Valid NTP Outgoing UDP Port
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      INCLUDES ANY:
        value: '123'
        field: Host-enabled_udp_outbound_ports
  towhat: Host
  file_mtime:
  guid: 1cb7f0ba-fa55-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000052
  notes: This condition verifies that the outgoing UDP port required by NTP (port
    123) is open.
- MiqPolicy:
  name: 04db603c-fa3a-11de-83ca-005056ba0614
  description: Firewall - Outgoing Security Level
  expression:
  towhat: Host
  guid: 04db603c-fa3a-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that only a defined set of outgoing TCP and UDP Ports
    are open.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}

```

```

Condition:
- name: f0afd7d6-fa3a-11de-83ca-005056ba0614
  description: Valid Outgoing TCP Ports
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      LIMITED TO:
        value: '902,427,443,27000,27010'
        field: Host-enabled_tcp_outbound_ports
  towhat: Host
  file_mtime:
  guid: f0afd7d6-fa3a-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 100000000000020
  notes: This condition verifies that the only open outgoing TCP ports are ↔
    427,443,902,27000,
    and 27010.
- name: 1778fb28-fa44-11de-83ca-005056ba0614
  description: Valid Outgoing UDP Ports
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      LIMITED TO:
        value: '427,123,902'
        field: Host-enabled_udp_outbound_ports
  towhat: Host
  file_mtime:
  guid: 1778fb28-fa44-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 100000000000020
  notes: This condition verifies that the only open outgoing UDP ports are 123,427,
    and 902.
- MiqPolicy:
  name: 2d6bfc2c-fa3b-11de-83ca-005056ba0614
  description: Limit Log Size
  expression:
  towhat: Vm
  guid: 2d6bfc2c-fa3b-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes:
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: vm_compliance_check
    description: VM Compliance Check
    guid: 816a598a-f57d-11de-a41a-005056ba0614
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant

```

```

    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: 8b9cf076-fa3b-11de-83ca-005056ba0614
    description: Log Size Limit <= 100KB
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkall:
            <=:
              value: '100000'
              field: Vm.advanced_settings-value
          search:
            =:
              value: log.rotateSize
              field: Vm.advanced_settings-name
        towhat: Vm
        file_mtime:
          guid: 8b9cf076-fa3b-11de-83ca-005056ba0614
          filename:
            applies_to_exp:
              miq_policy_id: 100000000000061
          notes:
- MiqPolicy:
  name: f1af8b44-fa3b-11de-83ca-005056ba0614
  description: Limit Number of Log Files
  expression:
  towhat: Vm
  guid: f1af8b44-fa3b-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes:
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: vm_compliance_check
    description: VM Compliance Check
    guid: 816a598a-f57d-11de-a41a-005056ba0614
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: f2ad72ac-fa3d-11de-83ca-005056ba0614
    description: Number of Log Files to Keep <= 10
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:

```

```

      FIND:
        checkall:
          <=:
            value: '10'
            field: Vm.advanced_settings-value
        search:
          =:
            value: log.keepOld
            field: Vm.advanced_settings-name
    towhat: Vm
    file_mtime:
    guid: f2ad72ac-fa3d-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000060
    notes:
- MiqPolicy:
  name: 2cd1b736-fa52-11de-83ca-005056ba0614
  description: Limit Software and Services Running in Service Console
  expression:
  towhat: Host
  guid: 2cd1b736-fa52-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy validates that only an approved list of services are enabled
    at boot time on an ESX host.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
  - name: c4c80bfa-fa55-11de-83ca-005056ba0614
    description: Default Services Running in Service Console
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        LIMITED TO:
          value: crond, firewall, gpm, ipmi, irqbalance, mgmt-vmware, microcode_ctl,
            mptctlnode, network, ntpd, pegasus, portmap, random, rawdevices, sshd,
            syslog, vmware, vmware-autostart, vmware-late, vmware-vmkauthd, vmware-vpxa,
            vmware-webAccess, wsman, xinetd
          field: Host-enabled_run_level_3_services
    towhat: Host
    file_mtime:

```

```

    guid: c4c80bfa-fa55-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000051
    notes: This conditions validates that a defined list of services are enabled
           with the ESX host is booted with networking support (run level 3). This list
           includes the generic services included in ESX. Additional hardware specific
           services can be added to the expression.
- MiqPolicy:
  name: 8cecc84c-fa46-11de-83ca-005056ba0614
  description: Limit su Access to root Account
  expression:
  towhat: Host
  guid: 8cecc84c-fa46-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy validates that only members of the group wheel can access the
        su command.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
  - name: 63b243fc-fa47-11de-83ca-005056ba0614
    description: Only members of wheel group can execute su command
    modifier: allow
    expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^\s*auth\s+required\s+.*pam_wheel\.so\s+use_uid
            field: Host.filesystems-contents
          search:
            =:
            value: /etc/pam.d/su
            field: Host.filesystems-name
    towhat: Host
    file_mtime:
    guid: 63b243fc-fa47-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000050
    notes: This condition validates that the file /etc/pam.d/su contains a variation

```

```

    of the string "auth required pam_wheel.so use_uid".
- MiqPolicy:
  name: c79821fa-fa53-11de-83ca-005056ba0614
  description: Limit vmkernel Size
  expression:
  towhat: Host
  guid: c79821fa-fa53-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy checks the vmkernel log is limited to a specified size.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
  - name: be9722e0-fa53-11de-83ca-005056ba0614
    description: vmkernel Log Size <= 4096KB
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:
              value: ^\s*size\s+(409[0-6]|40[0-8][0-9]|[123][0-9]{3}|\d{1,3})k
              field: Host.filesystems-contents
          search:
            =:
              value: /etc/logrotate.d/vmkernel
              field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: be9722e0-fa53-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 10000000000049
        notes: This condition verifies that the file /etc/logrotate.d/vmkernel is configured
              to limit the associated log to 4096KB.
- MiqPolicy:
  name: fc63df74-fa52-11de-83ca-005056ba0614
  description: Limit vmksummary Size
  expression:
  towhat: Host
  guid: fc63df74-fa52-11de-83ca-005056ba0614
  created_by: admin

```

```

updated_by: admin
notes: This policy checks the vmksummary log is limited to a specified size.
active: true
mode: compliance
MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
Condition:
- name: def33840-fa52-11de-83ca-005056ba0614
  description: vmksummary Log Size <= 4096KB
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^\s*size\s+(409[0-6]|40[0-8][0-9]|[123][0-9]{3}|\d{1,3})k
            field: Host.filesystems-contents
          search:
            =:
              value: /etc/logrotate.d/vmksummary
              field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: def33840-fa52-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 10000000000056
        notes: This condition verifies that the file /etc/logrotate.d/vmksummary is
          configured to limit the associated log to 4096KB.
- MiqPolicy:
  name: 79548666-fa51-11de-83ca-005056ba0614
  description: Limit vmkwarning Size
  expression:
  towhat: Host
  guid: 79548666-fa51-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy checks the vmkwarning log is limited to a specified size.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:

```

```

    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
    Condition:
-   name: 14d35e46-fa52-11de-83ca-005056ba0614
    description: vmkwarning Log Size <= 4096KB
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:
              value: ^\s*size\s+(409[0-6]|40[0-8][0-9]|[123][0-9]{3}|\d{1,3})k
              field: Host.filesystems-contents
          search:
            =:
              value: /etc/logrotate.d/vmkwarning
              field: Host.filesystems-name
      towhat: Host
      file_mtime:
      guid: 14d35e46-fa52-11de-83ca-005056ba0614
      filename:
      applies_to_exp:
      miq_policy_id: 100000000000048
      notes: This condition verifies that the file /etc/logrotate.d/vmkwarning is
        configured to limit the associated log to 4096KB.
-   MiqPolicy:
      name: b218c83c-c01c-11e3-b785-001a4a0f459e
      description: MyNew VM Control Policy
      expression:
      towhat: Vm
      guid: b218c83c-c01c-11e3-b785-001a4a0f459e
      created_by: admin
      updated_by: admin
      notes:
      active: true
      mode: control
      MiqPolicyContent:
      -   qualifier: success
          success_sequence: 1
          success_synchronous: true
      MiqEvent:
        name: vm_retired
        description: VM Retired
        guid: e363d8aa-1e1e-11de-8918-0050568005db
        event_type: Default
        definition:
          default:
          enabled:

```



```

    MiqAction:
      name: raise_automation_event
      description: Raise Automation Event
      guid: e7da3b7a-1139-11e1-9333-005056af009e
      action_type: default
      options: {}
    Condition: []
- MiqPolicy:
  name: 61b355f2-fee1-11de-83dd-005056ba5e76
  description: Network - Forged Transmits Must Be Disabled
  expression:
  towhat: Host
  guid: 61b355f2-fee1-11de-83dd-005056ba5e76
  created_by: admin
  updated_by: admin
  notes: This policy insures that forged transmits are disabled on both vLans and
    vSwitches.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: f246e3e0-fee1-11de-83dd-005056ba5e76
    description: Forged Transmits Disabled in vLan
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        not:
          CONTAINS:
            value: 'false'
            field: Host.lans-forged_transmits
    towhat: Host
    file_mtime:
    guid: f246e3e0-fee1-11de-83dd-005056ba5e76
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000022
    notes: This condition verifies that forged transmits are disabled on vlans.
  - name: a3ac5774-fee1-11de-83dd-005056ba5e76
    description: Forged Transmits Disabled in vSwitch
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        not:

```

```

      CONTAINS:
        value: 'false'
        field: Host.switches-forged_transmits
    towhat: Host
    file_mtime:
    guid: a3ac5774-fee1-11de-83dd-005056ba5e76
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000022
    notes: This condition verifies that forged transmits are disabled on vSwitches.
- MiqPolicy:
  name: de683aa6-fedf-11de-83dd-005056ba5e76
  description: Network - Mac Changes not Allowed
  expression:
  towhat: Host
  guid: de683aa6-fedf-11de-83dd-005056ba5e76
  created_by: admin
  updated_by: admin
  notes: This policy checks that MAC changes are not allowed on vSwitches and vLans.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
  - name: 0a6eb332-fee0-11de-83dd-005056ba5e76
    description: Mac Changes Disabled in vSwitches
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        not:
          CONTAINS:
            value: 'false'
            field: Host.switches-mac_changes
    towhat: Host
    file_mtime:
    guid: 0a6eb332-fee0-11de-83dd-005056ba5e76
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000028
    notes: This condition verifies that MAC changes are not allowed on vSwitches.
  - name: 3ed9fb4a-fee0-11de-83dd-005056ba5e76
    description: Mac Changes Disabled in vLans
    modifier: allow
    expression: !ruby/object:MiqExpression

```

```

    exp:
      not:
        CONTAINS:
          value: 'false'
          field: Host.lans-mac_changes
    towhat: Host
    file_mtime:
    guid: 3ed9fb4a-fee0-11de-83dd-005056ba5e76
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000028
    notes: This condition verifies that MAC changes are not allowed on vLans.
- MiqPolicy:
  name: 7cc14778-fe0f-11de-83dd-005056ba5e76
  description: Network - Promiscuous Mode Setting Not Disabled
  expression:
  towhat: Host
  guid: 7cc14778-fe0f-11de-83dd-005056ba5e76
  created_by: admin
  updated_by: admin
  notes: Check the Host VLAN setting for Promiscuous Mode which should be disabled.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
  - name: 2045b314-fe58-11de-83dd-005056ba5e76
    description: Check Host vSwitch - Promiscuous Mode Must Not Be Enable
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        not:
          CONTAINS:
            value: 'true'
            field: Host.switches-allow_promiscuous
    towhat: Host
    file_mtime:
    guid: 2045b314-fe58-11de-83dd-005056ba5e76
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000029
    notes: This condition verifies that vSwitches do not allow Promiscuous mode
      via inheritance.
  - name: 80e5ff5e-fe16-11de-83dd-005056ba5e76

```

```

description: Check Host Port - Promiscuous Mode Must Not Be Enabled
modifier: allow
expression: !ruby/object:MiqExpression
  exp:
    not:
      CONTAINS:
        value: 'true'
        field: Host.lans-computed_allow_promiscuous
towhat: Host
file_mtime:
guid: 80e5ff5e-fe16-11de-83dd-005056ba5e76
filename:
applies_to_exp:
miq_policy_id: 10000000000029
notes: This condition verifies that vLans do not allow Promiscuous mode via
  inheritance.
- MiqPolicy:
  name: Configuration Policy Restrict Cloning SQL Server
  description: ! 'Operational: Prevent Cloning of Database VMs'
  expression:
  towhat: Vm
  guid: 39fdeba0-2866-11de-af2a-0050568026c2
  created_by:
  updated_by: admin
  notes: prevents cloning of vms with a workload tag value of database
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_clone_start
      description: VM Clone Start
      guid: e30f6720-1e1e-11de-8918-0050568005db
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: cancel_task
      description: Cancel vCenter Task
      guid: e49bfee6-1e1e-11de-8918-0050568005db
      action_type: default
      options: {}
  - qualifier: success
    success_sequence: 2
    MiqEvent:
      name: vm_clone_start
      description: VM Clone Start
      guid: e30f6720-1e1e-11de-8918-0050568005db
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: SendEmail
      description: SendEmail
      guid: abcf406c-02cd-11de-86d4-005056903dbc
      action_type: email

```

[illegible]

```

      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    :value: Clone Prevented for SQL Server VM
    :attribute: EVM Policy
Condition:
- name: VMs running SQL Server
  description: VMs with Workload - Database
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      CONTAINS:
        tag: Vm.managed-function
        value: database
      context_type:
    towhat: Vm
    file_mtime:
    guid: 121ecf62-01c6-11de-a701-005056903dbc
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000064
    notes:
- MiqPolicy:
  name: Automation Policy - Scope VM Retirement Warning,  ResponseExecute Automation
  Model
  description: ! 'Operational: Retirement Warning'
  expression:
  towhat: Vm
  guid: 39621392-2866-11de-af2a-0050568026c2
  created_by:
  updated_by: admin
  notes: This policy raises an automation event when a retirement warning event
    is raised
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    failure_synchronous: true
  MiqEvent:

```

```

    name: vm_retire_warn
    description: VM Retirement Warning
    guid: 97c85330-fe93-11dd-b5e1-005056903dbc
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: raise_automation_event
    description: Raise Automation Event
    guid: e7da3b7a-1139-11e1-9333-005056af009e
    action_type: default
    options: {}
  Condition: []
- MiqPolicy:
  name: Automation Policy - Scope VM Retired Response Execute Automation Model
  description: ! 'Operational: Vm Retired'
  expression:
  towhat: Vm
  guid: 397700ae-2866-11de-af2a-0050568026c2
  created_by:
  updated_by: admin
  notes: This policy raises an automation event when a vm retirement event is raised
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    failure_synchronous: true
  MiqEvent:
    name: vm_retired
    description: VM Retired
    guid: e363d8aa-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: raise_automation_event
    description: Raise Automation Event
    guid: e7da3b7a-1139-11e1-9333-005056af009e
    action_type: default
    options: {}
  Condition: []
- MiqPolicy:
  name: 2f9fad14-fa4e-11de-83ca-005056ba0614
  description: Password Aging - Default Maximum
  expression:
  towhat: Host
  guid: 2f9fad14-fa4e-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy validates the ESX host's maximum password age configuration.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:

```

```

    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
    Condition:
- name: a4a0e740-fa4e-11de-83ca-005056ba0614
  description: Default Maximum Password Age <= 90days
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^\s*PASS_MAX_DAYS\s+([0-9]|[1-8][0-9]|90)
            field: Host.filesystems-contents
          search:
            =:
              value: /etc/login.defs
              field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: a4a0e740-fa4e-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 10000000000047
        notes: This condition checks the file /etc/login.defs and verifies that the
              PASS_MAX_DAYS parameter's value is 90 days or greater.
- MiqPolicy:
  name: 32b26f2c-fa4f-11de-83ca-005056ba0614
  description: Password Aging - Default Minimum
  expression:
  towhat: Host
  guid: 32b26f2c-fa4f-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy validates the ESX host's minimum password age configuration.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
    MiqAction:

```



```

    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
Condition:
- name: 79d39ad4-fa4f-11de-83ca-005056ba0614
  description: Default Minimum Password Age >= 0
  modifier: allow
  expression: !ruby/object:MiqExpression
  exp:
    FIND:
      checkany:
        REGULAR EXPRESSION MATCHES:
          value: ^\s*PASS_MIN_DAYS\s+\d+
          field: Host.filesystems-contents
      search:
        =:
          value: /etc/login.defs
          field: Host.filesystems-name
  towhat: Host
  file_mtime:
  guid: 79d39ad4-fa4f-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 100000000000059
  notes: This condition checks the file /etc/login.defs and verifies that the
    PASS_MIN_DAYS parameter's value is greater than or equal to 0 days.
- MiqPolicy:
  name: 305e6832-fa51-11de-83ca-005056ba0614
  description: Password Complexity - Minimum Length
  expression:
  towhat: Host
  guid: 305e6832-fa51-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies the minimum password length.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
Condition:
- name: c0ba559e-fa51-11de-83ca-005056ba0614
  description: Minimum Password Length >= 8

```

```

    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:
              value: ^\s*PASS_MIN_LEN\s+([8-9]|[1-9][0-9]+)
              field: Host.filesystems-contents
          search:
            =:
              value: /etc/login.defs
              field: Host.filesystems-name
    towhat: Host
    file_mtime:
    guid: c0ba559e-fa51-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000057
    notes: This condition checks the file /etc/login.defs and verifies that the
           PASS_MIN_LEN parameter's value is 8 or greater.
- MiqPolicy:
  name: 40b796dc-fa50-11de-83ca-005056ba0614
  description: Password Expiration Warning Default
  expression:
  towhat: Host
  guid: 40b796dc-fa50-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies the default setting for password expiration warning.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: 0e842bde-fa51-11de-83ca-005056ba0614
    description: Password Expiration Warning Default >= 7days
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:
              value: ^\s*PASS_WARN_AGE\s+([7-9]|[1-9][0-9]+)
              field: Host.filesystems-contents

```

```

      search:
        =:
          value: /etc/login.defs
          field: Host.filesystems-name
    towhat: Host
    file_mtime:
    guid: 0e842bde-fa51-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000046
    notes: This condition checks the file /etc/login.defs and verifies that PASS_WARN_AGE
      parameter's value is set to 7 or greater.
- MiqPolicy:
  name: e6f082ba-fa4c-11de-83ca-005056ba0614
  description: Password checking enabled for sudo
  expression:
  towhat: Host
  guid: e6f082ba-fa4c-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that password checking is enabled for sudo.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: 3d2074e2-fa4d-11de-83ca-005056ba0614
    description: NOPASSWD does not exist in sudoers file
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION DOES NOT MATCH:
              value: /^[^#]*NOPASSWD/i
              field: Host.filesystems-contents
          search:
            =:
              value: /etc/sudoers
              field: Host.filesystems-name
    towhat: Host
    file_mtime:
    guid: 3d2074e2-fa4d-11de-83ca-005056ba0614
    filename:

```

```

    applies_to_exp:
    miq_policy_id: 100000000000058
    notes: This condition check the file /etc/sudoers and verifies that it does
           not contain the word NOPASSWORD on an uncommented line.
- MiqPolicy:
  name: c5d44cb2-4734-11df-b577-005056a7121f
  description: ! 'Patch: MS10-008 Required'
  expression: !ruby/object:MiqExpression
    exp:
      CONTAINS:
        tag: Vm.managed-environment
        value: prod
      context_type:
  towhat: Vm
  guid: c5d44cb2-4734-11df-b577-005056a7121f
  created_by: admin
  updated_by: admin
  notes: Prevents a VM that does not have MS10-008 installed from running in the
         virtual environment. It's scope limits it to vms tagged as production
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: vm_start
      description: VM Power On
      guid: 404b4630-21a8-11e2-b47a-0050568b19a3
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: vm_stop
      description: Stop Virtual Machine
      guid: 37f2da3e-21a8-11e2-b47a-0050568b19a3
      action_type: default
      options: {}
  - qualifier: failure
    failure_sequence: 2
    MiqEvent:
      name: vm_start
      description: VM Power On
      guid: 404b4630-21a8-11e2-b47a-0050568b19a3
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: SendEmail
      description: SendEmail
      guid: abcf406c-02cd-11de-86d4-005056903dbc
      action_type: email
      options:
        :variables:
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''

```

```

      :oid: ''
      :var_type: <None>
-   :value: ''
      :oid: ''
      :var_type: <None>
-   :value: ''
      :oid: ''
      :var_type: <None>
-   :value: ''
      :oid: ''
      :var_type: <None>
-   :value: ''
      :oid: ''
      :var_type: <None>
-   :value: ''
      :oid: ''
      :var_type: <None>
-   :value: ''
      :oid: ''
      :var_type: <None>
      :from: evmadmin@manageiq.com
      :to: evm_demo@manageiq.com
-   qualifier: failure
      failure_sequence: 3
MiqEvent:
  name: vm_start
  description: VM Power On
  guid: 404b4630-21a8-11e2-b47a-0050568b19a3
  event_type: Default
  definition:
  default:
  enabled:
MiqAction:
  name: 722d25cc-56dc-11df-bb16-005056a7121f
  description: VM Attribute - Fails patch policy
  guid: 722d25cc-56dc-11df-bb16-005056a7121f
  action_type: set_custom_attribute
  options:
    :variables:
  -   :value: ''
      :oid: ''
      :var_type: <None>
  -   :value: ''
      :oid: ''
      :var_type: <None>
  -   :value: ''
      :oid: ''
      :var_type: <None>
  -   :value: ''
      :oid: ''
      :var_type: <None>
  -   :value: ''
      :oid: ''
      :var_type: <None>
  -   :value: ''
      :oid: ''

```

```

      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    :value: Failed Windows Required Patch Policy
    :attribute: EVM Policy
Condition:
- name: a3089008-4734-11df-b577-005056a7121f
  description: Verify KB978262 is installed
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      CONTAINS:
        value: KB978262
        field: Vm.patches-name
      context_type:
        towhat: Vm
        file_mtime:
          guid: a3089008-4734-11df-b577-005056a7121f
          filename:
            applies_to_exp:
              miq_policy_id: 10000000000071
            notes:
- MiqPolicy:
  name: e4c93c82-fa3a-11de-83ca-005056ba0614
  description: Permissions - /etc/grub.conf
  expression:
  towhat: Host
  guid: e4c93c82-fa3a-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that editing the server's boot process requires root
    level authority.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
        enabled:
  MiqAction:

```

```

    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
Condition:
- name: d2adb400-fa3b-11de-83ca-005056ba0614
  description: Permissions - /etc/grub.conf
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      and:
        - FIND:
            checkany:
              =:
                value: '0600'
                field: Host.filesystems-permissions
            search:
              =:
                value: /etc/grub.conf
                field: Host.filesystems-name
        - FIND:
            checkany:
              =:
                value: root
                field: Host.filesystems-owner
            search:
              =:
                value: /etc/grub.conf
                field: Host.filesystems-name
      towhat: Host
      file_mtime:
        guid: d2adb400-fa3b-11de-83ca-005056ba0614
      filename:
        applies_to_exp:
        miq_policy_id: 10000000000027
      notes: This condition verifies that the file /etc/grub.conf's permissions are
        set to 0600 and is owned by root.
- MiqPolicy:
    name: 7ea7db8c-fa46-11de-83ca-005056ba0614
    description: Permissions - /etc/snmp/snmpd.conf
    expression:
    towhat: Host
    guid: 7ea7db8c-fa46-11de-83ca-005056ba0614
    created_by: admin
    updated_by: admin
    notes: This policy ensures that access to SNMP configuration parameters are limited
      to the root user.
    active: true
    mode: compliance
    MiqPolicyContent:
      - qualifier: failure
        failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:

```

```

    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: ebb24a50-fa46-11de-83ca-005056ba0614
    description: Permissions - /etc/snmp/snmpd.conf
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        and:
        - FIND:
            checkany:
              =:
                value: '0700'
                field: Host.filesystems-permissions
            search:
              =:
                value: /etc/snmp/snmpd.conf
                field: Host.filesystems-name
        - FIND:
            checkany:
              =:
                value: root
                field: Host.filesystems-owner
            search:
              =:
                value: /etc/snmp/snmpd.conf
                field: Host.filesystems-name
      towhat: Host
      file_mtime:
      guid: ebb24a50-fa46-11de-83ca-005056ba0614
      filename:
      applies_to_exp:
      miq_policy_id: 10000000000045
      notes: This condition verifies that the permissions of /etc/snmp/snmpd.conf
        are 0700 and is owned by root.
  - MiqPolicy:
      name: 7408efa8-21b3-11e2-a38c-0050568b19a3
      description: Power-Off Virtual Machines
      expression:
      towhat: Vm
      guid: 7408efa8-21b3-11e2-a38c-0050568b19a3
      created_by: admin
      updated_by: admin
      notes:
      active: true
      mode: control
      MiqPolicyContent:
      - qualifier: success
        success_sequence: 1
      MiqEvent:
        name: vm_start
        description: VM Power On
        guid: 404b4630-21a8-11e2-b47a-0050568b19a3

```



```

    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: vm_stop
    description: Stop Virtual Machine
    guid: 37f2da3e-21a8-11e2-b47a-0050568b19a3
    action_type: default
    options: {}
  Condition:
- name: d514b2fa-21b3-11e2-a38c-0050568b19a3
  description: VM with Workload Tag Messaging
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      !binary "Q090VEFJTlM=":
      !binary "dGFn": Vm.managed-function
      !binary "dmFsdWU=": messaging
    context_type:
  towhat: Vm
  file_mtime:
  guid: d514b2fa-21b3-11e2-a38c-0050568b19a3
  filename:
  applies_to_exp:
  miq_policy_id:
  notes:
- MiqPolicy:
  name: f4f0e916-bbd5-11e1-a4a4-005056b25af6
  description: Prevent PowerOn of Quarantined VM
  expression:
  towhat: Vm
  guid: f4f0e916-bbd5-11e1-a4a4-005056b25af6
  created_by: admin
  updated_by: admin
  notes:
  active: true
  mode: control
  MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: request_vm_start
    description: VM Power On Request
    guid: 48b02c4a-ae7c-11e1-a76f-005056b25af6
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: vm_stop
    description: Stop Virtual Machine
    guid: 37f2da3e-21a8-11e2-b47a-0050568b19a3
    action_type: default
    options: {}
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_start

```

```

    description: VM Power On
    guid: 404b4630-21a8-11e2-b47a-0050568b19a3
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: vm_stop
    description: Stop Virtual Machine
    guid: 37f2da3e-21a8-11e2-b47a-0050568b19a3
    action_type: default
    options: {}
  Condition:
- name: 1cbc27da-bbd6-11e1-ac0c-005056b25af6
  description: VM Tagged as Do Not PowerOn
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      CONTAINS:
        tag: Vm.managed-exclusions
        value: do_not_power_on
      context_type:
  towhat: Vm
  file_mtime:
  guid: 1cbc27da-bbd6-11e1-ac0c-005056b25af6
  filename:
  applies_to_exp:
  miq_policy_id:
  notes:
- MiqPolicy:
  name: eb84f288-fa39-11de-83ca-005056ba0614
  description: Protect Root File System Filling /home
  expression:
  towhat: Host
  guid: eb84f288-fa39-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that the /home directory is mounted on a different
    partition than the root filesystem.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:

```

```

- name: 62447a1a-fa3a-11de-83ca-005056ba0614
  description: Protect Root File System Filling /home
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^[^\#]*\home
            field: Host.filesystems-contents
          search:
            =:
              value: /etc/fstab
              field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: 62447a1a-fa3a-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 10000000000019
        notes: This condition verifies that the file /etc/fstab has an uncommented line
              that references the directory /home.
- MiqPolicy:
  name: a128d356-fa36-11de-83ca-005056ba0614
  description: Protect Root File System Filling /tmp
  expression:
  towhat: Host
  guid: a128d356-fa36-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that the /tmp directory is mounted on a different
        partition than the root filesystem.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
      default:
      enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
  - name: 267dd9de-fa37-11de-83ca-005056ba0614
    description: Protect Root File System Filling /tmp
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:

```

```

      REGULAR EXPRESSION MATCHES:
        value: ^[^\#]*\tmp
        field: Host.filesystems-contents
    search:
      =:
        value: /etc/fstab
        field: Host.filesystems-name
  towhat: Host
  file_mtime:
  guid: 267dd9de-fa37-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000044
  notes: This condition verifies that the file /etc/fstab has an uncommented line
    that references the directory /tmp.
- MiqPolicy:
  name: 854d45aa-fa3a-11de-83ca-005056ba0614
  description: Protect Root File System Filling /var/log
  expression:
  towhat: Host
  guid: 854d45aa-fa3a-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that the /var/log directory is mounted on a different
    partition than the root filesystem.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
  - name: a84173e2-fa3a-11de-83ca-005056ba0614
    description: Protect Root File System Filling /var/log
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:
              value: ^[^\#]*\var\log
              field: Host.filesystems-contents
          search:
            =:
              value: /etc/fstab
              field: Host.filesystems-name

```

```

    towhat: Host
    file_mtime:
    guid: a84173e2-fa3a-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000055
    notes: This condition verifies that the file /etc/fstab has an uncommented line
           that references the directory /var/log.
- MiqPolicy:
  name: 57189108-d1d3-11e1-9ede-005056af009e
  description: Record Last RDP User
  expression:
  towhat: Vm
  guid: 57189108-d1d3-11e1-9ede-005056af009e
  created_by: admin
  updated_by: admin
  notes: ! 'When a user logs on to the VM through an RDP session, the file c:\rdp_login\rdp. ←
         log
         is automatically created by the logon script.

A analysis profile should be set to retrieve this file and its content.

This policy will automatically raise an automate event so the content of the
file can be parsed and elements set as custom attributes of the VM '
active: true
mode: control
MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_scan_complete
    description: VM Analysis Complete
    guid: f7b8361e-1139-11e1-9333-005056af009e
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: raise_automation_event
    description: Raise Automation Event
    guid: e7da3b7a-1139-11e1-9333-005056af009e
    action_type: default
    options: {}
Condition:
- name: 5a4c3456-de30-11e1-9088-005056af009e
  description: Check for files starting with rep
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkcount:
          ! '>=':
            field: <count>
            value: '1'
        search:
          INCLUDES:
            field: Vm.filesystems-name

```

```

        value: rdp
        context_type:
        towhat: Vm
        file_mtime:
        guid: 5a4c3456-de30-11e1-9088-005056af009e
        filename:
        applies_to_exp:
        miq_policy_id: 4
        notes:
- MiqPolicy:
  name: 5ce6be9a-fa4c-11de-83ca-005056ba0614
  description: Require users to enter own password - no ROOTPW entry
  expression:
  towhat: Host
  guid: 5ce6be9a-fa4c-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that when the sudo command is used, each user is prompted
    for their password and not the root password.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
- name: a791b882-fa4c-11de-83ca-005056ba0614
  description: ROOTPW does not exist in sudoers file
  modifier: allow
  expression: !ruby/object:MiqExpression
  exp:
    FIND:
      checkany:
        REGULAR EXPRESSION DOES NOT MATCH:
          value: /^[^#]*ROOTPW/i
          field: Host.filesystems-contents
      search:
        =:
          value: /etc/sudoers
          field: Host.filesystems-name
  towhat: Host
  file_mtime:
  guid: a791b882-fa4c-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000043

```

```

    notes: This condition check the file /etc/sudoers and verifies that it does
           not contain the word ROOTPW on an uncommented line.
- MiqPolicy:
  name: a3a56370-c015-11e3-b785-001a4a0f459e
  description: Retirement of VM
  expression: !ruby/object:MiqExpression
    exp:
      =:
        field: Vm-retired
        value: 'true'
    context_type:
  towhat: Vm
  guid: a3a56370-c015-11e3-b785-001a4a0f459e
  created_by: admin
  updated_by: admin
  notes:
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    success_synchronous: true
  MiqEvent:
    name: vm_retired
    description: VM Retired
    guid: e363d8aa-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: vm_retire
    description: Retire Virtual Machine
    guid: 047c677e-431c-11e3-91d5-001a4a0f459e
    action_type: default
    options: {}
  Condition: []
- MiqPolicy:
  name: eb0151ea-fa47-11de-83ca-005056ba0614
  description: Root Login on console should be Disabled
  expression:
  towhat: Host
  guid: eb0151ea-fa47-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that the root account cannot directly login via the
        console.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:

```

```

    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: 571e6e76-fa48-11de-83ca-005056ba0614
    description: File /etc/securetty should be empty
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkall:
            =:
              value: '0'
              field: Host.filesystems-size
          search:
            =:
              value: /etc/securetty
              field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: 571e6e76-fa48-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 10000000000026
        notes: This condition checks the file /etc/securetty and verifies that it's
          empty by checking for a 0KB file size.
  - MiqPolicy:
    name: c63b0560-fa45-11de-83ca-005056ba0614
    description: Root Login via SSH should be Disabled
    expression:
    towhat: Host
    guid: c63b0560-fa45-11de-83ca-005056ba0614
    created_by: admin
    updated_by: admin
    notes: This policy verifies that the root account cannot login to the host via
      SSH.
    active: true
    mode: compliance
    MiqPolicyContent:
    - qualifier: failure
      failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}

```



```

Condition:
- name: 4435b6d6-fa46-11de-83ca-005056ba0614
  description: PermitRootLogin = no in sshd_config file
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^\s*PermitRootLogin\s+no
            field: Host.filesystems-contents
        search:
          =:
            value: /etc/ssh/sshd_config
            field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: 4435b6d6-fa46-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 100000000000042
        notes: This condition checks the file /etc/ssh/sshd_config and verifies that
              the PermitRootLogin parameter's value is set to no.
- MiqPolicy:
  name: 24b92088-399c-11de-ae27-005056a11a54
  description: Service Level Gold - RAM must be 1GB and 1 vCPU - off
  expression: !ruby/object:MiqExpression
    exp:
      and:
        - CONTAINS:
            tag: Vm.managed-service_level
            value: gold
        - =:
            value: 'off'
            field: Vm-power_state
      context_type:
    towhat: Vm
    guid: 24b92088-399c-11de-ae27-005056a11a54
    created_by:
    updated_by: admin
    notes: This policy verifies that a vm that has a service level tag of gold has
          1vCPU and 1GB of memory. If not it changes the vm to these values. This policy
          is used on a powered off vm.
    active: true
    mode: control
    MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: assigned_company_tag
      description: Tag Complete
      guid: e384ecb6-1e1e-11de-8918-0050568005db
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: VM_RAM_1GB
      description: Set VM RAM to 1GB

```

```

    guid: 2d8445f2-9aec-11dd-8e55-005056ac7d2c
    action_type: reconfigure_memory
    options:
      :value: 1024
- qualifier: success
  success_sequence: 2
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: VM_CPU_1
    description: Set VM CPU to 1
    guid: d97dafba-9af1-11dd-8e55-005056ac7d2c
    action_type: reconfigure_cpus
    options:
      :value: '1'
  Condition:
- name: 1c6ec35e-3908-11de-b6d5-005056a11a54
  description: Service Level Gold - VM RAM and CPU check
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      or:
      - ! '!=':
          value: 1024
          field: Vm.hardware-memory_cpu
      - ! '!=':
          value: 1
          field: Vm.hardware-numvcpus
    towhat: Vm
    file_mtime:
    guid: 1c6ec35e-3908-11de-b6d5-005056a11a54
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000069
    notes:
- MiqPolicy:
  name: 7a91f3ac-3908-11de-b6d5-005056a11a54
  description: Service Level Gold - RAM must be 1GB and 1 vCPU - on
  expression: !ruby/object:MiqExpression
    exp:
      and:
      - CONTAINS:
          tag: Vm.managed-service_level
          value: gold
      - =:
          value: 'on'
          field: Vm-power_state
    context_type:
    towhat: Vm
    guid: 7a91f3ac-3908-11de-b6d5-005056a11a54
    created_by:
    updated_by: admin
    notes: This policy verifies that a vm that has a service level tag of gold has

```

```
1vCPU and 1GB of memory. If not it changes the vm to these values. This policy
is used on a powered on vm.
active: true
mode: control
MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: vm_stop
    description: Stop Virtual Machine
    guid: 37f2da3e-21a8-11e2-b47a-0050568b19a3
    action_type: default
    options: {}
- qualifier: success
  success_sequence: 2
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: VM_RAM_1GB
    description: Set VM RAM to 1GB
    guid: 2d8445f2-9aec-11dd-8e55-005056ac7d2c
    action_type: reconfigure_memory
    options:
      :value: 1024
- qualifier: success
  success_sequence: 3
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: VM_CPU_1
    description: Set VM CPU to 1
    guid: d97dafba-9af1-11dd-8e55-005056ac7d2c
    action_type: reconfigure_cpus
    options:
      :value: '1'
- qualifier: success
  success_sequence: 4
  MiqEvent:
    name: assigned_company_tag
```

```

    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: vm_start
    description: Start Virtual Machine
    guid: 55b5a422-3348-11de-bde2-005056a170fa
    action_type: default
    options: {}
  Condition:
- name: 1c6ec35e-3908-11de-b6d5-005056a11a54
  description: Service Level Gold - VM RAM and CPU check
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      or:
      - ! '!=':
          value: 1024
          field: Vm.hardware-memory_cpu
      - ! '!=':
          value: 1
          field: Vm.hardware-numvcpus
  towhat: Vm
  file_mtime:
  guid: 1c6ec35e-3908-11de-b6d5-005056a11a54
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000069
  notes:
- MiqPolicy:
  name: b265c970-3908-11de-b6d5-005056a11a54
  description: Service Level Platinum - RAM must be 2GB and 2 vCPUs - off
  expression: !ruby/object:MiqExpression
    exp:
      and:
      - CONTAINS:
          tag: Vm.managed-service_level
          value: platinum
      - =:
          value: 'off'
          field: Vm-power_state
    context_type:
  towhat: Vm
  guid: b265c970-3908-11de-b6d5-005056a11a54
  created_by:
  updated_by: admin
  notes: This policy verifies that a vm that has a service level tag of platinum
    has 2 vCPUs and 2GB of memory. If not it changes the vm to these values. This
    policy is used on a powered off vm.
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
  MiqEvent:
    name: assigned_company_tag

```

```

    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: VM_RAM_2GB
    description: Set VM RAM to 2GB
    guid: cf1570b2-9af1-11dd-8e55-005056ac7d2c
    action_type: reconfigure_memory
    options:
      :value: 2048
- qualifier: success
  success_sequence: 2
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: VM_CPU_2
    description: Set VM CPU to 2
    guid: e2c3d64e-9af1-11dd-8e55-005056ac7d2c
    action_type: reconfigure_cpus
    options:
      :value: '2'
  Condition:
- name: 34218558-3909-11de-b6d5-005056a11a54
  description: Service Level Platinum - VM RAM and CPU check
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      or:
        - ! '!=':
            value: 2048
            field: Vm.hardware-memory_cpu
        - ! '!=':
            value: 2
            field: Vm.hardware-numvcpus
    towhat: Vm
    file_mtime:
    guid: 34218558-3909-11de-b6d5-005056a11a54
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000070
    notes:
- MiqPolicy:
  name: 4cb4d05c-3909-11de-b6d5-005056a11a54
  description: Service Level Platinum - RAM must be 2GB and 2 vCPUs - on
  expression: !ruby/object:MiqExpression
    exp:
      and:
        - CONTAINS:
            tag: Vm.managed-service_level
            value: platinum

```

```

    - =:
      value: 'on'
      field: Vm-power_state
    context_type:
  towhat: Vm
  guid: 4cb4d05c-3909-11de-b6d5-005056a11a54
  created_by:
  updated_by: admin
  notes: This policy verifies that a vm that has a service level tag of platinum
    has 2 vCPUs and 2GB of memory. If not it changes the vm to these values. This
    policy is used on a powered on vm.
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: assigned_company_tag
      description: Tag Complete
      guid: e384ecb6-1e1e-11de-8918-0050568005db
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: vm_stop
      description: Stop Virtual Machine
      guid: 37f2da3e-21a8-11e2-b47a-0050568b19a3
      action_type: default
      options: {}
  - qualifier: success
    success_sequence: 2
    MiqEvent:
      name: assigned_company_tag
      description: Tag Complete
      guid: e384ecb6-1e1e-11de-8918-0050568005db
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: VM_RAM_2GB
      description: Set VM RAM to 2GB
      guid: cf1570b2-9af1-11dd-8e55-005056ac7d2c
      action_type: reconfigure_memory
      options:
        :value: 2048
  - qualifier: success
    success_sequence: 3
    MiqEvent:
      name: assigned_company_tag
      description: Tag Complete
      guid: e384ecb6-1e1e-11de-8918-0050568005db
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: VM_CPU_2

```

```

    description: Set VM CPU to 2
    guid: e2c3d64e-9af1-11dd-8e55-005056ac7d2c
    action_type: reconfigure_cpus
    options:
      :value: '2'
- qualifier: success
  success_sequence: 4
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1ele-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: vm_start
    description: Start Virtual Machine
    guid: 55b5a422-3348-11de-bde2-005056a170fa
    action_type: default
    options: {}
  Condition:
- name: 34218558-3909-11de-b6d5-005056a11a54
  description: Service Level Platinum - VM RAM and CPU check
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      or:
      - ! '!=':
          value: 2048
          field: Vm.hardware-memory_cpu
      - ! '!=':
          value: 2
          field: Vm.hardware-numvcpus
  towhat: Vm
  file_mtime:
  guid: 34218558-3909-11de-b6d5-005056a11a54
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000070
  notes:
- MiqPolicy:
  name: Service Level Policy Verify Virtual Hardware - Silver Level
  description: Service Level Silver - RAM must be 512MB and 1 vCPU - off
  expression: !ruby/object:MiqExpression
    exp:
      and:
      - CONTAINS:
          tag: Vm.managed-service_level
          value: silver
      - =:
          value: 'off'
          field: Vm-power_state
  context_type:
  towhat: Vm
  guid: 3659b8bc-2866-11de-af2a-0050568026c2
  created_by:
  updated_by: admin
  notes: This policy verifies that a vm that has a service level tag of silver has

```

```

    1 vCPU and 512MB of memory. If not it changes the vm to these values. This policy
    is used on a powered off vm.
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: assigned_company_tag
      description: Tag Complete
      guid: e384ecb6-1ele-11de-8918-0050568005db
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: VM_CPU_1
      description: Set VM CPU to 1
      guid: d97dafba-9af1-11dd-8e55-005056ac7d2c
      action_type: reconfigure_cpus
      options:
        :value: '1'
  - qualifier: success
    success_sequence: 2
    MiqEvent:
      name: assigned_company_tag
      description: Tag Complete
      guid: e384ecb6-1ele-11de-8918-0050568005db
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: VM_RAM_512MB
      description: Set VM RAM to 512MB
      guid: bab04cb4-9af1-11dd-8e55-005056ac7d2c
      action_type: reconfigure_memory
      options:
        :value: 512
  Condition:
  - name: Service Level Validation Silver - Powered Off
    description: Service Level Silver - VM RAM and CPU check
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        or:
        - ! '!=':
            value: 512
            field: Vm.hardware-memory_cpu
        - ! '!=':
            value: 1
            field: Vm.hardware-numvcpus
  towhat: Vm
  file_mtime:
  guid: 531575ae-9b1c-11dd-bbd7-005056ac7d2c
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000068
  notes:

```



```

- MiqPolicy:
  name: d16643b6-3905-11de-b6d5-005056a11a54
  description: Service Level Silver - RAM must be 512MB and 1 vCPU - on
  expression: !ruby/object:MiqExpression
    exp:
      and:
        - CONTAINS:
            tag: Vm.managed-service_level
            value: silver
        - =:
            value: 'on'
            field: Vm-power_state
      context_type:
    towhat: Vm
  guid: d16643b6-3905-11de-b6d5-005056a11a54
  created_by:
  updated_by: admin
  notes: This policy verifies that a vm that has a service level tag of silver has
    1 vCPU and 512MB of memory. If not it changes the vm to these values. This policy
    is used on a powered on vm.
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: assigned_company_tag
      description: Tag Complete
      guid: e384ecb6-1e1e-11de-8918-0050568005db
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: vm_stop
      description: Stop Virtual Machine
      guid: 37f2da3e-21a8-11e2-b47a-0050568b19a3
      action_type: default
      options: {}
  - qualifier: success
    success_sequence: 2
    MiqEvent:
      name: assigned_company_tag
      description: Tag Complete
      guid: e384ecb6-1e1e-11de-8918-0050568005db
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: VM_RAM_512MB
      description: Set VM RAM to 512MB
      guid: bab04cb4-9af1-11dd-8e55-005056ac7d2c
      action_type: reconfigure_memory
      options:
        :value: 512
  - qualifier: success
    success_sequence: 3
    MiqEvent:

```

```

    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
MiqAction:
  name: VM_CPU_1
  description: Set VM CPU to 1
  guid: d97dafba-9af1-11dd-8e55-005056ac7d2c
  action_type: reconfigure_cpus
  options:
    :value: '1'
- qualifier: success
  success_sequence: 4
MiqEvent:
  name: assigned_company_tag
  description: Tag Complete
  guid: e384ecb6-1e1e-11de-8918-0050568005db
  event_type: Default
  definition:
    default:
    enabled:
MiqAction:
  name: vm_start
  description: Start Virtual Machine
  guid: 55b5a422-3348-11de-bde2-005056a170fa
  action_type: default
  options: {}
Condition:
- name: Service Level Validation Silver - Powered Off
  description: Service Level Silver - VM RAM and CPU check
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      or:
        - ! '!=':
            value: 512
            field: Vm.hardware-memory_cpu
        - ! '!=':
            value: 1
            field: Vm.hardware-numvcpus
    towhat: Vm
    file_mtime:
    guid: 531575ae-9b1c-11dd-bbd7-005056ac7d2c
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000068
    notes:
- MiqPolicy:
  name: 498f5330-fa4b-11de-83ca-005056ba0614
  description: Settings - Remote syslog Logging
  expression:
  towhat: Host
  guid: 498f5330-fa4b-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that syslog is configured to utilize a remote server.

```

```

active: true
mode: compliance
MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
Condition:
- name: ee09af6e-fa4b-11de-83ca-005056ba0614
  description: Verify syslog Utilizes a Remote Host
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: /^[^#*]\s*.*@/
            field: Host.filesystems-contents
          search:
            =:
              value: /etc/syslog.conf
              field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: ee09af6e-fa4b-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 10000000000025
        notes: This condition checks the file /etc/syslog.conf and verifies the existence
              of the @ parameter, which is used to specify the use of a remote server.
- MiqPolicy:
  name: c340f524-fa3e-11de-83ca-005056ba0614
  description: Settings - /etc/grub.conf
  expression:
  towhat: Host
  guid: c340f524-fa3e-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that a password is required in order to edit the server's
        boot process.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check

```

```

    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
    default:
    enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
    Condition:
  - name: 1f18225a-fa3f-11de-83ca-005056ba0614
    description: Verify /etc/grub.conf Settings
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:
              value: ^\s*password\s\-\-md5
              field: Host.filesystems-contents
          search:
            =:
              value: /etc/grub.conf
              field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: 1f18225a-fa3f-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 10000000000041
        notes: This condition check the file /etc/grub.conf and verifies that the parameter
              "password --md5" exists.
  - MiqPolicy:
      name: e3f6428c-a85a-11e3-9c44-001a4a0f459e
      description: Settings - /etc/resolv.conf
      expression: !ruby/object:MiqExpression
        exp:
          FIND:
            search:
              =:
                field: Vm.filesystems-name
                value: resolv.conf
            checkall:
              =:
                field: Vm.filesystems-contents_available
                value: 'true'
          context_type:
        towhat: Vm
        guid: e3f6428c-a85a-11e3-9c44-001a4a0f459e
        created_by: admin
        updated_by: admin
        notes:
        active: true
        mode: compliance
        MiqPolicyContent:
      - qualifier: success

```

```

    success_sequence: 1
    success_synchronous: true
  MiqEvent:
    name: vm_compliance_check
    description: VM Compliance Check
    guid: 816a598a-f57d-11de-a41a-005056ba0614
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: log
    description: Generate log message
    guid: 04771f80-431c-11e3-91d5-001a4a0f459e
    action_type: default
    options: {}
- qualifier: success
  success_sequence: 2
  success_synchronous: true
  MiqEvent:
    name: vm_compliance_check
    description: VM Compliance Check
    guid: 816a598a-f57d-11de-a41a-005056ba0614
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: c26b7988-a860-11e3-9c44-001a4a0f459e
    description: resolv.conf
    guid: c26b7988-a860-11e3-9c44-001a4a0f459e
    action_type: custom_automation
    options:
      :ae_request: resolvsend
      :ae_message: create
- qualifier: failure
  failure_sequence: 1
  failure_synchronous: true
  MiqEvent:
    name: vm_compliance_check
    description: VM Compliance Check
    guid: 816a598a-f57d-11de-a41a-005056ba0614
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: log
    description: Generate log message
    guid: 04771f80-431c-11e3-91d5-001a4a0f459e
    action_type: default
    options: {}
  Condition: []
- MiqPolicy:
  name: 6576a074-fa48-11de-83ca-005056ba0614
  description: Settings - /etc/sudoers
  expression:
  towhat: Host
  guid: 6576a074-fa48-11de-83ca-005056ba0614

```

```

created_by: admin
updated_by: admin
notes: This policy verifies that sudo is configured to use syslog for logging.
active: true
mode: compliance
MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
- name: ade186c6-fa48-11de-83ca-005056ba0614
  description: Verify sudo is Logging via syslog
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^\s*Defaults\s+syslog\=
            field: Host.filesystems-contents
          search:
            =:
              value: /etc/sudoers
              field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: ade186c6-fa48-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 10000000000040
        notes: This condition check the file /etc/sudoers and verifies that the parameter
              "Defaults syslog=" exists.
- MiqPolicy:
  name: ab373d88-fa4a-11de-83ca-005056ba0614
  description: Settings - Display Logs on Different Terminals
  expression:
  towhat: Host
  guid: ab373d88-fa4a-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that critical, error, and warning level log messages
        are directed to distinct terminals.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure

```

```

failure_sequence: 1
MiqEvent:
  name: host_compliance_check
  description: Host Compliance Check
  guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
  event_type: Default
  definition:
    default:
    enabled:
MiqAction:
  name: compliance_failed
  description: Mark as Non-Compliant
  guid: ba452d94-f586-11de-8ebc-0050568a07c7
  action_type: default
  options: {}
Condition:
- name: f383ec6c-fa4a-11de-83ca-005056ba0614
  description: Verify Different Logs Displayed on Different Terminals
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      and:
        - FIND:
            checkany:
              REGULAR EXPRESSION MATCHES:
                value: ^\s*\*\.crit\s+\/dev\/tty
                field: Host.filesystems-contents
            search:
              =:
                value: /etc/syslog.conf
                field: Host.filesystems-name
        - FIND:
            checkany:
              REGULAR EXPRESSION MATCHES:
                value: ^\s*\*\.err\s+\/dev\/tty
                field: Host.filesystems-contents
            search:
              =:
                value: /etc/syslog.conf
                field: Host.filesystems-name
        - FIND:
            checkany:
              REGULAR EXPRESSION MATCHES:
                value: ^\s*\*\.warning\s+\/dev\/tty
                field: Host.filesystems-contents
            search:
              =:
                value: /etc/syslog.conf
                field: Host.filesystems-name
  towhat: Host
  file_mtime:
  guid: f383ec6c-fa4a-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000024
  notes: This condition checks the file /etc/syslog.conf has three seperate parameters
    defined for critical, error, and warning level log messages. These parameters
    specify the tty will display the specified log messages.
- MiqPolicy:

```

```

name: 4b188948-fa45-11de-83ca-005056ba0614
description: Settings - SNMP Read Only Access
expression:
towhat: Host
guid: 4b188948-fa45-11de-83ca-005056ba0614
created_by: admin
updated_by: admin
notes: This policy verifies that SNMP is configured to only allow read-only access.
active: true
mode: compliance
MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
Condition:
- name: e328c720-fa45-11de-83ca-005056ba0614
  description: SNMP Configured for Read-only Access
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      and:
        - FIND:
            checkany:
              REGULAR EXPRESSION MATCHES:
                value: ^\s*rocommunity
                field: Host.filesystems-contents
            search:
              =:
                value: /etc/snmp/snmpd.conf
                field: Host.filesystems-name
        - FIND:
            checkany:
              REGULAR EXPRESSION DOES NOT MATCH:
                value: ^\s*rwcommunity
                field: Host.filesystems-contents
            search:
              =:
                value: /etc/snmp/snmpd.conf
                field: Host.filesystems-name
  towhat: Host
  file_mtime:
  guid: e328c720-fa45-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000054
  notes: This condition checks the file /etc/snmp/snmpd.conf and verifies that

```



```

    the rocommunity parameter is defined and the rwcommunity parameter is not.
- MiqPolicy:
  name: 0864fae6-fa54-11de-83ca-005056ba0614
  description: Settings - vmkernel Compress Option
  expression:
  towhat: Host
  guid: 0864fae6-fa54-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that the vmkernel log is compressed by default.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
  - name: fe7378be-fa53-11de-83ca-005056ba0614
    description: Verify Compression Enabled in vmkernel
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:
              value: \s+compress
              field: Host.filesystems-contents
          search:
            =:
              value: /etc/logrotate.d/vmkernel
              field: Host.filesystems-name
    towhat: Host
    file_mtime:
    guid: fe7378be-fa53-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000039
    notes: This condition checks the file /etc/logrotate.d/vmkernel and verifies
           that the option compress is enabled.
- MiqPolicy:
  name: 6353b57e-fa53-11de-83ca-005056ba0614
  description: Settings - vmksummary Compress Option
  expression:
  towhat: Host
  guid: 6353b57e-fa53-11de-83ca-005056ba0614
  created_by: admin

```

```

updated_by: admin
notes: This policy verifies that the vmksummary log is compressed by default.
active: true
mode: compliance
MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
Condition:
- name: 510f7286-fa53-11de-83ca-005056ba0614
  description: Verify Compression Enabled in vmksummary
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: \s+compress
            field: Host.filesystems-contents
        search:
          =:
            value: /etc/logrotate.d/vmksummary
            field: Host.filesystems-name
      towhat: Host
      file_mtime:
      guid: 510f7286-fa53-11de-83ca-005056ba0614
      filename:
      applies_to_exp:
      miq_policy_id: 10000000000038
      notes: This condition checks the file /etc/logrotate.d/vmksummary and verifies
        that the option compress is enabled.
- MiqPolicy:
  name: 4614d62e-fa52-11de-83ca-005056ba0614
  description: Settings - vmkwarning Compress Option
  expression:
  towhat: Host
  guid: 4614d62e-fa52-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that the vmkwarning log is compressed by default.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:

```

```

    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
MiqAction:
  name: compliance_failed
  description: Mark as Non-Compliant
  guid: ba452d94-f586-11de-8ebc-0050568a07c7
  action_type: default
  options: {}
Condition:
- name: a51cbaba-fa52-11de-83ca-005056ba0614
  description: Verify Compression Enabled in vmkwarning
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: \s+compress
            field: Host.filesystems-contents
        search:
          =:
            value: /etc/logrotate.d/vmkwarning
            field: Host.filesystems-name
    towhat: Host
    file_mtime:
    guid: a51cbaba-fa52-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000037
    notes: This condition checks the file /etc/logrotate.d/vmkwarning and verifies
           that the option compress is enabled.
- MiqPolicy:
  name: 994efe7e-18e6-11e0-88b4-005056a7184a
  description: ! 'Snapshots: Delete based on Count'
  expression:
  towhat: Vm
  guid: 994efe7e-18e6-11e0-88b4-005056a7184a
  created_by: admin
  updated_by: admin
  notes: This policy deletes the most recent snapshot when more that 2 snapshots
        exists
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
  MiqEvent:
    name: vm_snapshot_complete
    description: VM Snapshot Create Complete
    guid: 7eb82802-135e-11e0-8706-005056a7184a
    event_type: Default
    definition:
      default:
      enabled:

```

```

    MiqAction:
      name: delete_most_recent_snapshot
      description: Delete Most Recent Snapshot
      guid: 7f6e2f8a-135e-11e0-8706-005056a7184a
      action_type: default
      options: {}
  Condition:
  - name: 992035fc-18e7-11e0-88b4-005056a7184a
    description: Check for more than 2 snapshots
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        ! '>':
          value: '2'
          field: Vm-v_total_snapshots
      context_type:
        towhat: Vm
        file_mtime:
          guid: 992035fc-18e7-11e0-88b4-005056a7184a
          filename:
            applies_to_exp:
              miq_policy_id: 100000000000075
            notes: Checks to see if more than 2 snapshots exist
  - MiqPolicy:
      name: cf87e7fc-99d8-11e1-a4bf-005056b057a8
      description: ! 'Snapshots: limit to max of 2'
      expression:
        towhat: Vm
      guid: cf87e7fc-99d8-11e1-a4bf-005056b057a8
      created_by: admin
      updated_by: admin
      notes: This policy prevents a vm from starting if there are more than 2 snapshots.
        If this number is exceeded, the vm is not allowed to start and the vm annotations
        are updated in the VC
      active: true
      mode: control
      MiqPolicyContent:
      - qualifier: success
        success_sequence: 1
        MiqEvent:
          name: vm_start
          description: VM Power On
          guid: 404b4630-21a8-11e2-b47a-0050568b19a3
          event_type: Default
          definition:
            default:
            enabled:
        MiqAction:
          name: vm_stop
          description: Stop Virtual Machine
          guid: 37f2da3e-21a8-11e2-b47a-0050568b19a3
          action_type: default
          options: {}
      - qualifier: success
        success_sequence: 2
        MiqEvent:
          name: vm_start
          description: VM Power On
          guid: 404b4630-21a8-11e2-b47a-0050568b19a3

```

```

    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: 8d6ebd90-99d9-11e1-a4bf-005056b057a8
    description: ! 'VM Attribute: Max Snapshots'
    guid: 8d6ebd90-99d9-11e1-a4bf-005056b057a8
    action_type: set_custom_attribute
    options:
      :value: Snapshot Limit Exceeded
      :attribute: EVM Policy
  Condition:
- name: 9db4783a-99d8-11e1-a4bf-005056b057a8
  description: Snapshot Count >=3
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      ! '>=':
        count: Vm.snapshots
        value: '3'
    context_type:
  towhat: Vm
  file_mtime:
  guid: 9db4783a-99d8-11e1-a4bf-005056b057a8
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000079
  notes: This condition checks to see if 3 or more snapshots exist
- MiqPolicy:
  name: 98557866-d2ee-11de-b4f6-0050568a547d
  description: ! 'Tag: Host Workload - DMZ'
  expression:
  towhat: Host
  guid: 98557866-d2ee-11de-b4f6-0050568a547d
  created_by: admin
  updated_by: admin
  notes: This policy will automatically apply a DMZ tag to a host if it has access
    to the external vlan
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
  MiqEvent:
    name: host_scan_complete
    description: Host Analysis Complete
    guid: ffcfb368-455d-11de-86a0-005056a81f62
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: 330828a4-d2ef-11de-b4f6-0050568a547d
    description: Tag as DMZ
    guid: 330828a4-d2ef-11de-b4f6-0050568a547d
    action_type: tag
    options:
      :tags:

```

```

    - /managed/network_location/dmz
Condition:
- name: ed3edf84-d2ee-11de-b4f6-0050568a547d
  description: Host - DMZ vlan check
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          IS NOT NULL:
            field: Host.lans-created_on
        search:
          INCLUDES:
            value: External
            field: Host.lans-name
      towhat: Host
      file_mtime:
      guid: ed3edf84-d2ee-11de-b4f6-0050568a547d
      filename:
      applies_to_exp:
      miq_policy_id: 10000000000017
      notes:
- MiqPolicy:
  name: 0c2517d8-1ea2-11e0-8e71-005056910000
  description: ! 'Tag: VM Inherit Cluster Location Tag'
  expression:
  towhat: Vm
  guid: 0c2517d8-1ea2-11e0-8e71-005056910000
  created_by: admin
  updated_by: admin
  notes: This policy allows a vm to inherit the location tag of it's parent cluster
    on creation or completion of analysis
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_create
      description: VM Create Complete
      guid: 4c0b4f12-37c0-11df-b567-005056a40709
      event_type: Default
      definition:
      default:
      enabled:
    MiqAction:
      name: 60e5d690-1ea2-11e0-8e71-005056910000
      description: ! 'Tag: Inherit Cluster Location Tag'
      guid: 60e5d690-1ea2-11e0-8e71-005056910000
      action_type: inherit_parent_tags
      options:
        :parent_type: ems_cluster
        :cats:
        - location
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_scan_complete
      description: VM Analysis Complete

```

```

    guid: f7b8361e-1139-11e1-9333-005056af009e
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: 60e5d690-1ea2-11e0-8e71-005056910000
    description: ! 'Tag: Inherit Cluster Location Tag'
    guid: 60e5d690-1ea2-11e0-8e71-005056910000
    action_type: inherit_parent_tags
    options:
      :parent_type: ems_cluster
      :cats:
      - location
  Condition: []
- MiqPolicy:
  name: 66fbec86-d2ef-11de-b4f6-0050568a547d
  description: ! 'Tag: VM Workload - DMZ'
  expression:
  towhat: Vm
  guid: 66fbec86-d2ef-11de-b4f6-0050568a547d
  created_by: admin
  updated_by: admin
  notes: This policy will automatically apply a DMZ tag to a vm if it has access
    to the external vlan
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
  MiqEvent:
    name: vm_scan_complete
    description: VM Analysis Complete
    guid: f7b8361e-1139-11e1-9333-005056af009e
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: 330828a4-d2ef-11de-b4f6-0050568a547d
    description: Tag as DMZ
    guid: 330828a4-d2ef-11de-b4f6-0050568a547d
    action_type: tag
    options:
      :tags:
      - /managed/network_location/dmz
  Condition:
  - name: 8a975658-d2ef-11de-b4f6-0050568a547d
    description: VM - DMZ check
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            IS NOT NULL:
              field: Vm.lans-created_on
          search:
            INCLUDES:
              value: External

```

```

        field: Vm.lans-name
    towhat: Vm
    file_mtime:
    guid: 8a975658-d2ef-11de-b4f6-0050568a547d
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000018
    notes:
- MiqPolicy:
  name: 07cea762-3d1b-11df-a7e9-005056a40709
  description: ! 'Tag: VM if Analysis not successful'
  expression:
  towhat: Vm
  guid: 07cea762-3d1b-11df-a7e9-005056a40709
  created_by: admin
  updated_by: admin
  notes:
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_scan_abort
      description: VM Analysis Failure
      guid: 4c48a6fa-37c0-11df-b567-005056a40709
      event_type: Default
      definition:
      default:
      enabled:
    MiqAction:
      name: fc7f2dde-3d22-11df-a7e9-005056a40709
      description: Tag VM that Fails Analysis
      guid: fc7f2dde-3d22-11df-a7e9-005056a40709
      action_type: tag
      options:
        :variables:
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>

```



```

      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    :tags:
    - /managed/operations/analysis_failed
  Condition: []
- MiqPolicy:
  name: 0ce6cf38-3d2d-11df-a7e9-005056a40709
  description: ! 'Tag: VM on Successful Analysis'
  expression:
  towhat: Vm
  guid: 0ce6cf38-3d2d-11df-a7e9-005056a40709
  created_by: admin
  updated_by: admin
  notes:
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_scan_complete
      description: VM Analysis Complete
      guid: f7b8361e-1139-11e1-9333-005056af009e
      event_type: Default
      definition:
      default:
      enabled:
    MiqAction:
      name: cd2f3222-3d2c-11df-a7e9-005056a40709
      description: Tag VM after Successful Analysis
      guid: cd2f3222-3d2c-11df-a7e9-005056a40709
      action_type: tag
      options:
      :tags:
      - /managed/operations/analysis_success
  Condition: []
- MiqPolicy:
  name: b968f0a0-3d2e-11df-a7e9-005056a40709
  description: ! 'Tag: VM that Requires Analysis'
  expression:
  towhat: Vm
  guid: b968f0a0-3d2e-11df-a7e9-005056a40709
  created_by: admin
  updated_by: admin
  notes:
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_start
      description: VM Power On

```

```

    guid: 404b4630-21a8-11e2-b47a-0050568b19a3
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: a4ccd026-3d2e-11df-a7e9-005056a40709
    description: Tag VM that Requires Analysis
    guid: a4ccd026-3d2e-11df-a7e9-005056a40709
    action_type: tag
    options:
      :tags:
      - /managed/operations/analysis_required
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_create
    description: VM Create Complete
    guid: 4c0b4f12-37c0-11df-b567-005056a40709
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: a4ccd026-3d2e-11df-a7e9-005056a40709
    description: Tag VM that Requires Analysis
    guid: a4ccd026-3d2e-11df-a7e9-005056a40709
    action_type: tag
    options:
      :tags:
      - /managed/operations/analysis_required
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_reset
    description: VM Reset
    guid: 4c1b8a3a-37c0-11df-b567-005056a40709
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: a4ccd026-3d2e-11df-a7e9-005056a40709
    description: Tag VM that Requires Analysis
    guid: a4ccd026-3d2e-11df-a7e9-005056a40709
    action_type: tag
    options:
      :tags:
      - /managed/operations/analysis_required
  Condition: []
- MiqPolicy:
  name: ccadf9fa-fa56-11de-83ca-005056ba0614
  description: Time Keeping - NTP Configured to Use Loopback Adapter
  expression:
  towhat: Host
  guid: ccadf9fa-fa56-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that NTP performs all name resolutions via a loopback

```

```

    network.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
  - name: 2b9bb8b2-fa57-11de-83ca-005056ba0614
    description: NTP Configured to Use Loopback Adapter
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:
              value: ^\s*restrict\s+127\.0\.0\.1
              field: Host.filesystems-contents
          search:
            =:
              value: /etc/ntp.conf
              field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: 2b9bb8b2-fa57-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 10000000000036
        notes: This condition checks the file /etc/ntp.conf and verifies that the restrict
          parameter's value is set to 127.0.0.1.
- MiqPolicy:
  name: ebc02cea-fa57-11de-83ca-005056ba0614
  description: Time Keeping - Restrict Access for Machines without Loopback
  expression:
  towhat: Host
  guid: ebc02cea-fa57-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that only non-loopback machines can access the NTP
    service.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:

```

```

    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
    Condition:
- name: ddc26260-fa58-11de-83ca-005056ba0614
  description: Access Restricted for Machines without Loopback
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^\s*restrict\s+default\s+kod\s+nomodify\s+notrap
            field: Host.filesystems-contents
        search:
          =:
            value: /etc/ntp.conf
            field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: ddc26260-fa58-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 100000000000035
        notes: This condition checks the file /etc/ntp.conf and verifies that the line
              "restrict default kod nomodify notrap" exists.
- MiqPolicy:
  name: 3819638c-fa57-11de-83ca-005056ba0614
  description: Timekeeping - Drift Enabled
  expression:
  towhat: Host
  guid: 3819638c-fa57-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that NTP's driftfile support is enabled.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
    MiqAction:

```

```

    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
Condition:
- name: 71fae5da-fa57-11de-83ca-005056ba0614
  description: Verify NTP Uses a Driftfile
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^\s*driftfile\s+\/var\/lib\/ntp\/drift
            field: Host.filesystems-contents
          search:
            =:
              value: /etc/ntp.conf
              field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: 71fae5da-fa57-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 100000000000034
        notes: This condition checks the file /etc/ntp.conf and verifies that the driftfile
          parameter exists.
- MiqPolicy:
  name: c4396f3a-fa55-11de-83ca-005056ba0614
  description: Timekeeping - Minimum of 3 NTP Servers Defined in hosts
  expression:
  towhat: Host
  guid: c4396f3a-fa55-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that a minimum of 3 NTP servers are defined in the
    local hosts file.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
Condition:
- name: 2698c39c-fa56-11de-83ca-005056ba0614

```

```

description: Verify 3 NTP Servers Defined in hosts File
modifier: allow
expression: !ruby/object:MiqExpression
  exp:
    FIND:
      checkany:
        RUBY:
          value: ! "count = 0\ncontext.each_line { |line|
            Break up the input by lines\n  count += 1 if line =~ /^[^#]*NTP/i
            \ # Increment Count if line matches our regular expression\n}\nreturn
            true if count >= 3\nreturn false\n"
          field: Host.filesystems-contents
        search:
          =:
            value: /etc/hosts
            field: Host.filesystems-name
        towhat: Host
      file_mtime:
        guid: 2698c39c-fa56-11de-83ca-005056ba0614
      filename:
        applies_to_exp:
        miq_policy_id: 100000000000033
      notes: ! 'This conditions checks the file /etc/hosts and veries that there are
        at least 3 uncommented lines that reference ntp servers. The included expression
        can be modified to match the appropriate values for the ntp servers for your
        environment.

```

```

,
- MiqPolicy:
  name: a6c2a51e-fa57-11de-83ca-005056ba0614
  description: Timekeeping - Minimum of 3 NTP Servers Defined in ntp.conf
  expression:
  towhat: Host
  guid: a6c2a51e-fa57-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that a minimum of 3 servers are defined in the NTP
    configuration.
  active: true
  mode: compliance
  MiqPolicyContent:
    - qualifier: failure
      failure_sequence: 1
      MiqEvent:
        name: host_compliance_check
        description: Host Compliance Check
        guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
        event_type: Default
        definition:
          default:
          enabled:
      MiqAction:
        name: compliance_failed
        description: Mark as Non-Compliant
        guid: ba452d94-f586-11de-8ebc-0050568a07c7
        action_type: default
        options: {}
  Condition:
    - name: 03c821bc-fa58-11de-83ca-005056ba0614

```

```

description: Verify 3 NTP Servers Defined in ntp.conf
modifier: allow
expression: !ruby/object:MiqExpression
  exp:
    FIND:
      checkany:
        RUBY:
          value: ! "count = 0\ncontext.each_line { |line|
            Break up the input by lines\n  count += 1 if line =~ /^[^#]*server\\s+[0-9A- ↵
              Za-z]*/
            \  # Increment Count if line matches our regular expression\n}\nreturn
              true if count >= 3\nreturn false"
          field: Host.filesystems-contents
        search:
          =:
            value: /etc/ntp.conf
            field: Host.filesystems-name
        towhat: Host
      file_mtime:
      guid: 03c821bc-fa58-11de-83ca-005056ba0614
      filename:
      applies_to_exp:
      miq_policy_id: 10000000000032
      notes: This condition checks the file /etc/ntp.conf and verifies that a minimum
        of three ntp servers are defined.
- MiqPolicy:
  name: 8d4a7bee-fa56-11de-83ca-005056ba0614
  description: Timekeeping - Minimum of 3 NTP Servers defined in step-tickers
  expression:
  towhat: Host
  guid: 8d4a7bee-fa56-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that a minimum of 3 servers are defined in the NTP
    step-tickers configuration.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: 0806448a-fa57-11de-83ca-005056ba0614
    description: Verify 3 NTP Servers Defined in step-tickers File
    modifier: allow
    expression: !ruby/object:MiqExpression

```

```

exp:
  FIND:
    checkany:
      RUBY:
        value: ! "count = 0\ncontext.each_line { |line|
          Break up the input by lines\n  count += 1 if line =~ /^[^#]*server\\s+[0-9A- ↵
          Za-z]+/
          \  # Increment Count if line matches our regular expression\n)\nreturn
          true if count >= 3\nreturn false\n"
        field: Host.filesystems-contents
      search:
        =:
          value: /etc/ntp/step-tickers
          field: Host.filesystems-name
    towhat: Host
    file_mtime:
    guid: 0806448a-fa57-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000023
    notes: This condition checks the file /etc/ntp/step-tickers and verifies that
      a minimum of three ntp servers are defined.
- MiqPolicy:
  name: 4ed279b2-fa55-11de-83ca-005056ba0614
  description: Timekeeping - NTP Service Running
  expression:
  towhat: Host
  guid: 4ed279b2-fa55-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that the NTP servers is configured to automatically
    start.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: 9a08d21e-fa55-11de-83ca-005056ba0614
    description: Verify NTP is Running
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:

```



```

      INCLUDES:
        value: '3'
        field: Host.host_services-enable_run_levels
      search:
        =:
          value: ntpd
          field: Host.host_services-name
      towhat: Host
      file_mtime:
      guid: 9a08d21e-fa55-11de-83ca-005056ba0614
      filename:
      applies_to_exp:
      miq_policy_id: 10000000000031
      notes: This condition verifies that the run level of the service ntpd is set
        to three.
- MiqPolicy:
  name: a8e0ef7c-fa48-11de-83ca-005056ba0614
  description: Use sudo aliases
  expression:
  towhat: Host
  guid: a8e0ef7c-fa48-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that user aliases are enabled in the configuration
    of the sudo command.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
  - name: 99496ebc-fa49-11de-83ca-005056ba0614
    description: Aliases are being used for sudo authorization
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:
              value: ^\s*User_Alias
              field: Host.filesystems-contents
          search:
            =:
              value: /etc/sudoers
              field: Host.filesystems-name

```

```

    towhat: Host
    file_mtime:
    guid: 99496ebc-fa49-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000030
    notes: This condition checks the file /etc/sudoers and verifies that the parameter
           "User_Alias" is defined.
- MiqPolicy:
  name: 2cd19756-c1ec-11e1-ae68-000c29cc1a4c
  description: VMWare SHG v4.x & v5.x - VMX01 - Prevent virtual disk shrinking.
  expression: !ruby/object:MiqExpression
    exp:
      =:
        value: VMware
        field: Vm-vendor
    context_type:
  towhat: Vm
  guid: 2cd19756-c1ec-11e1-ae68-000c29cc1a4c
  created_by: admin
  updated_by: admin
  notes: VMWare SHG v4.x & v5.x - VMX01 - Prevent virtual disk shrinking. R1
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: vm_compliance_check
    description: VM Compliance Check
    guid: 816a598a-f57d-11de-a41a-005056ba0614
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: 11564bce-c1ed-11e1-ae68-000c29cc1a4c
    description: VMWare SHG v4.x - VMX01 - Prevent virtual disk shrinking
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        and:
        - FIND:
            checkany:
              =:
                field: Vm.advanced_settings-value
                value: 'true'
            search:
              =:
                field: Vm.advanced_settings-name
                value: isolation.tools.diskShrink.disable
        - FIND:
            checkany:

```

```

      =:
        field: Vm.advanced_settings-value
        value: 'true'
    search:
      =:
        field: Vm.advanced_settings-name
        value: isolation.tools.diskWiper.disable
    context_type:
  towhat: Vm
  file_mtime:
  guid: 11564bce-clcd-11e1-ae68-000c29cc1a4c
  filename:
  applies_to_exp: !ruby/object:MiqExpression
  exp:
    STARTS WITH:
      value: '4'
      field: Vm.host-vmm_version
    context_type:
  miq_policy_id: 13
  notes: VMWare SHG v4.x - VMX01 - Prevent virtual disk shrinking R1
- name: d4bd19f4-d7d6-11e1-b3e5-000c2999f7f1
  description: VMWare SHG v5.x - VMX01 - Prevent virtual disk shrinking
  modifier: allow
  expression: !ruby/object:MiqExpression
  exp:
    FIND:
      checkany:
        =:
          field: Vm.advanced_settings-value
          value: 'true'
        search:
          =:
            field: Vm.advanced_settings-name
            value: isolation.tools.diskWiper.disable
          context_type:
        towhat: Vm
        file_mtime:
        guid: d4bd19f4-d7d6-11e1-b3e5-000c2999f7f1
        filename:
        applies_to_exp: !ruby/object:MiqExpression
        exp:
          STARTS WITH:
            field: Vm.host-vmm_version
            value: '5'
          context_type:
        miq_policy_id: 13
        notes: VMWare SHG v5.x - VMX01 - Prevent virtual disk shrinking R1
- MiqPolicy:
  name: 774404fc-clcd-11e1-ae68-000c29cc1a4c
  description: VMWare SHG v4.x & v5.x - VMX22 - Avoid using independent nonpersistent
    disks.
  expression: !ruby/object:MiqExpression
  exp:
    =:
      value: VMware
      field: Vm-vendor
    context_type:
  towhat: Vm
  guid: 774404fc-clcd-11e1-ae68-000c29cc1a4c

```

```

created_by: admin
updated_by: admin
notes: VMWare SHG v4.x & v5.x - VMX22 - Avoid using independent nonpersistent
  disks.
active: true
mode: compliance
MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: vm_compliance_check
    description: VM Compliance Check
    guid: 816a598a-f57d-11de-a41a-005056ba0614
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
- name: b6c3548e-c1c1-11e1-ae68-000c29cc1a4c
  description: VMWare SHG v4.x & v5.x - VMX22 - Avoid using independent nonpersistent
    disks.
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkcount:
          =:
            value: '0'
            field: <count>
        search:
          INCLUDES:
            value: independent_nonpersistent
            field: Vm.hardware.disks-mode
        context_type:
      towhat: Vm
      file_mtime:
      guid: b6c3548e-c1c1-11e1-ae68-000c29cc1a4c
      filename:
      applies_to_exp:
      miq_policy_id: 3
      notes: VMWare SHG v4.x & v5.x - VMX22 - Avoid using independent nonpersistent
        disks. R1
- MiqPolicy:
  name: 5e3a568e-cfe3-11e1-986c-000c29cc1a4c
  description: VMWare SHG v4.x & v5.x - VSH05 - Install VMware vCenter Server using
    a service account
  expression: !ruby/object:MiqExpression
    exp:
      CONTAINS:
        field: Vm.win32_services-name
        value: vpxd
      context_type:
      towhat: Vm

```

```

guid: 5e3a568e-cfe3-11e1-986c-000c29cc1a4c
created_by: admin
updated_by: admin
notes: VMWare SHG v4.x & v5.x - VSH05 - Install VMware vCenter Server using a
  service account R1
active: true
mode: compliance
MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: vm_compliance_check
    description: VM Compliance Check
    guid: 816a598a-f57d-11de-a41a-005056ba0614
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
Condition:
- name: 9e841928-cfe8-11e1-986c-000c29cc1a4c
  description: VMWare SHG v4.x & v5.x - VSH05 - Install VMware vCenter Server
    using a service account
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION DOES NOT MATCH:
            field: Vm.win32_services-object_name
            value: \bLocalSystem
        search:
          =:
            field: Vm.win32_services-name
            value: vpxd
        context_type:
        towhat: Vm
        file_mtime:
        guid: 9e841928-cfe8-11e1-986c-000c29cc1a4c
        filename:
        applies_to_exp:
        miq_policy_id: 4
        notes: VMWare SHG v4.x & v5.x - VSH05 - Install VMware vCenter Server using
          a service account R1
- MiqPolicy:
  name: 17fce8ee-c39f-11e1-aed6-000c29cc1a4c
  description: VMware SHG - VMX24 - Disable certain unexposed features.
  expression:
  towhat: Vm
  guid: 17fce8ee-c39f-11e1-aed6-000c29cc1a4c
  created_by: admin
  updated_by: admin
  notes: VMware SHG - VMX24 - Disable certain unexposed features.
  active: true

```

```
mode: compliance
MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: vm_compliance_check
    description: VM Compliance Check
    guid: 816a598a-f57d-11de-a41a-005056ba0614
    event_type: Default
    definition:
      default:
        enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
Condition:
- name: 98427d34-c39f-11e1-aed6-000c29cc1a4c
  description: Disable certain unexposed features
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      and:
        - FIND:
            checkany:
              =:
                field: Vm.advanced_settings-value
                value: 'true'
            search:
              =:
                field: Vm.advanced_settings-name
                value: isolation.tools.unity.push.update.disable
        - FIND:
            checkany:
              =:
                field: Vm.advanced_settings-value
                value: 'true'
            search:
              =:
                field: Vm.advanced_settings-name
                value: isolation.tools.ghi.launchmenu.change
        - FIND:
            checkany:
              =:
                field: Vm.advanced_settings-value
                value: 'true'
            search:
              =:
                field: Vm.advanced_settings-name
                value: isolation.tools.memSchedFakeSampleStats.disable
        - FIND:
            checkany:
              =:
                field: Vm.advanced_settings-value
                value: 'true'
            search:
              =:
```

```

        field: Vm.advanced_settings-name
        value: isolation.tools.getCreds.disable
    context_type:
    towhat: Vm
    file_mtime:
    guid: 98427d34-c39f-11e1-aed6-000c29cc1a4c
    filename:
    applies_to_exp:
    miq_policy_id: 1
    notes:
- MiqPolicy:
  name: e5871bee-d435-11e1-9935-000c2999f7f1
  description: VMware SHG v4.x & v5.x - HCN05 - Disable DCUI to prevent all local
    administrative control
  expression: !ruby/object:MiqExpression
  exp:
    =:
      value: ESXi
      field: Host-vmx_product
  context_type:
  towhat: Host
  guid: e5871bee-d435-11e1-9935-000c2999f7f1
  created_by: admin
  updated_by: admin
  notes: VMware SHG v4.x & v5.x - HCN05 - Disable DCUI to prevent all local administrative
    control R1
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: 0f6761b2-d436-11e1-9935-000c2999f7f1
    description: VMware SHG v4.x & v5.x - HCN05 - Disable DCUI to prevent all local
      administrative control
    modifier: allow
    expression: !ruby/object:MiqExpression
    exp:
      FIND:
      checkall:
      =:
        value: 'false'
        field: Host.host_services-running
      search:
      =:

```

```

        value: DCUI
        field: Host.host_services-name
    context_type:
    towhat: Host
    file_mtime:
    guid: 0f6761b2-d436-11e1-9935-000c2999f7f1
    filename:
    applies_to_exp:
    miq_policy_id: 14
    notes: VMware SHG v4.x & v5.x - HCN05 - Disable DCUI to prevent all local administrative
        control R1
- MiqPolicy:
  name: 3a2acbde-d434-11e1-9935-000c2999f7f1
  description: VMware SHG v4.x & v5.x - HCN06 - Disable Tech Support Mode unless
    needed for diagnostics and break-fix
  expression: !ruby/object:MiqExpression
  exp:
    =:
      field: Host-vmx_product
      value: ESXi
  context_type:
  towhat: Host
  guid: 3a2acbde-d434-11e1-9935-000c2999f7f1
  created_by: admin
  updated_by: admin
  notes: VMware SHG v4.x & v5.x - HCN06 - Disable Tech Support Mode unless needed
    for diagnostics and break-fix R1
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: e35c1be0-d434-11e1-9935-000c2999f7f1
    description: VMware SHG v4.x & v5.x - HCN06 - Disable Tech Support Mode unless
      needed for diagnostics and break-fix
    modifier: allow
    expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkall:
        =:
          field: Host.host_services-running
          value: 'false'
        search:

```



```

      =:
        field: Host.host_services-name
        value: TSM
      context_type:
    towhat: Host
    file_mtime:
    guid: e35c1be0-d434-11e1-9935-000c2999f7f1
    filename:
    applies_to_exp:
    miq_policy_id: 15
    notes: VMware SHG v4.x & v5.x - HCN06 - Disable Tech Support Mode unless needed
      for diagnostics and break-fix R1
- MiqPolicy:
  name: 36021318-d435-11e1-9935-000c2999f7f1
  description: VMware SHG v4.x & v5.x - HCN07 - Set a timeout for Tech Support Mode.
  expression: !ruby/object:MiqExpression
  exp:
    =:
      field: Host-vmx_product
      value: ESXi
    context_type:
  towhat: Host
  guid: 36021318-d435-11e1-9935-000c2999f7f1
  created_by: admin
  updated_by: admin
  notes: VMware SHG v4.x & v5.x - HCN07 - Set a timeout for Tech Support Mode. R1
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
  - name: 9f3b5376-d435-11e1-9935-000c2999f7f1
    description: VMware SHG v4.x - HCN07 - Set a timeout for Tech Support Mode.
    modifier: allow
    expression: !ruby/object:MiqExpression
    exp:
      not:
        FIND:
          checkall:
            =:
              field: Host.advanced_settings-value
              value: '0'
          search:
            =:

```

```

        field: Host.advanced_settings-name
        value: UserVars.TSMTIMEOUT
      context_type:
      towhat: Host
      file_mtime:
      guid: 9f3b5376-d435-11e1-9935-000c2999f7f1
      filename:
      applies_to_exp: !ruby/object:MiqExpression
      exp:
        STARTS WITH:
          field: Host-vmm_version
          value: '4'
        context_type:
      miq_policy_id: 5
      notes: VMware SHG v4.x - HCN07 - Set a timeout for Tech Support Mode. R1
- name: fc017d86-d7cf-11e1-b3e5-000c2999f7f1
  description: VMware SHG v5.x - HCN07 - Set a timeout for Tech Support Mode.
  modifier: allow
  expression: !ruby/object:MiqExpression
  exp:
    not:
      FIND:
        checkall:
          =:
            value: '0'
            field: Host.advanced_settings-value
        search:
          =:
            value: UserVars.ESXiShellTimeout
            field: Host.advanced_settings-name
    context_type:
    towhat: Host
    file_mtime:
    guid: fc017d86-d7cf-11e1-b3e5-000c2999f7f1
    filename:
    applies_to_exp: !ruby/object:MiqExpression
    exp:
      STARTS WITH:
        value: '5'
        field: Host-vmm_version
      context_type:
    miq_policy_id: 5
    notes: VMware SHG v5.x - HCN07 - Set a timeout for Tech Support Mode. R1
- MiqPolicy:
  name: 4dadd9bc-d443-11e1-9935-000c2999f7f1
  description: VMware SHG v4.x & v5.x - HLG01 - Remote syslog should be configured
  expression: !ruby/object:MiqExpression
  exp:
    =:
      value: ESXi
      field: Host-vmm_product
    context_type:
    towhat: Host
    guid: 4dadd9bc-d443-11e1-9935-000c2999f7f1
    created_by: admin
    updated_by: admin
    notes: VMware SHG v4.x & v5.x - HLG01 - Remote syslog should be configured
    active: true
    mode: compliance

```

```

MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
- name: b60247d2-d443-11e1-9935-000c2999f7f1
  description: VMware SHG v5.x - HLG01 - Remote syslog should be configured
  modifier: allow
  expression: !ruby/object:MiqExpression
  exp:
    FIND:
      checkall:
        IS NOT EMPTY:
          value: ''
          field: Host.advanced_settings-value
      search:
        =:
          value: Syslog.global.logHost
          field: Host.advanced_settings-name
    context_type:
  towhat: Host
  file_mtime:
  guid: b60247d2-d443-11e1-9935-000c2999f7f1
  filename:
  applies_to_exp: !ruby/object:MiqExpression
  exp:
    STARTS WITH:
      field: Host-vmm_version
      value: '5'
    context_type:
  miq_policy_id: 6
  notes: VMware SHG - HLG01 - Remote syslog should be configured VERSION 5.x ONLY
  R1
- name: 456a882a-d7ce-11e1-b3e5-000c2999f7f1
  description: VMware SHG v4.x - HLG01 - Remote syslog should be configured
  modifier: allow
  expression: !ruby/object:MiqExpression
  exp:
    FIND:
      checkall:
        IS NOT EMPTY:
          field: Host.advanced_settings-value
          value: ''
      search:
        =:
          field: Host.advanced_settings-name

```

```

      value: Syslog.Remote.Hostname
    context_type:
    towhat: Host
    file_mtime:
    guid: 456a882a-d7ce-11e1-b3e5-000c2999f7f1
    filename:
    applies_to_exp: !ruby/object:MiqExpression
      exp:
        STARTS WITH:
          field: Host-vmm_version
          value: '4'
        context_type:
    miq_policy_id: 6
    notes: VMware SHG - HLG01 - Remote syslog should be configured VERSION 4.x ONLY
    R1
- MiqPolicy:
  name: 197d032e-d016-11e1-986c-000c29cc1a4c
  description: ! "VMware SHG v4.x & v5.x - NCN03 - Ensure that the \x80\x9CMAC
    Address Change\x80\x9D policy is set to \x80\x9Creject.\x80\x9D"
  expression: !ruby/object:MiqExpression
    exp:
      =:
        value: ESXi
        field: Host-vmm_product
      context_type:
    towhat: Host
    guid: 197d032e-d016-11e1-986c-000c29cc1a4c
    created_by: admin
    updated_by: admin
    notes: ! "VMware SHG v4.x & v5.x - NCN03 - Ensure that the \x80\x9CMAC Address
      Change\x80\x9D policy is set to \x80\x9Creject.\x80\x9D R1"
    active: true
    mode: compliance
    MiqPolicyContent:
      - qualifier: failure
        failure_sequence: 1
      MiqEvent:
        name: host_compliance_check
        description: Host Compliance Check
        guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
        event_type: Default
        definition:
          default:
          enabled:
      MiqAction:
        name: compliance_failed
        description: Mark as Non-Compliant
        guid: ba452d94-f586-11de-8ebc-0050568a07c7
        action_type: default
        options: {}
    Condition:
      - name: 3531486e-d016-11e1-986c-000c29cc1a4c
        description: ! "VMware SHG v4.x & v5.x - NCN03 - Ensure that the \x80\x9CMAC
          Address Change\x80\x9D policy is set to \x80\x9Creject.\x80\x9D"
        modifier: allow
        expression: !ruby/object:MiqExpression
          exp:
            FIND:
              checkall:

```

```

      =:
        value: 'false'
        field: Host.lans-mac_changes
    search:
      IS NOT NULL:
        value: ''
        field: Host.lans-name
    context_type:
  towhat: Host
  file_mtime:
  guid: 3531486e-d016-11e1-986c-000c29cc1a4c
  filename:
  applies_to_exp:
  miq_policy_id: 7
  notes: ! "VMware SHG v4.x & v5.x - NCN03 - Ensure that the â\x80\x9CMAC Address
    Changeâ\x80\x9D policy is set to â\x80\x9Creject.â\x80\x9D R1"
- MiqPolicy:
  name: e4d7e0e6-d00e-11e1-986c-000c29cc1a4c
  description: ! "VMware SHG v4.x & v5.x - NCN04 - Ensure that the â\x80\x9CForged
    Transmitsâ\x80\x9D policy is set to â\x80\x9Creject.â\x80\x9D"
  expression: !ruby/object:MiqExpression
  exp:
    =:
      field: Host-vmm_product
      value: ESXi
    context_type:
  towhat: Host
  guid: e4d7e0e6-d00e-11e1-986c-000c29cc1a4c
  created_by: admin
  updated_by: admin
  notes: ! "VMware SHG v4.x & v5.x - NCN04 - Ensure that the â\x80\x9CForged Transmitsâ\x80\x9D ←
    x9D
    policy is set to â\x80\x9Creject.â\x80\x9D R1"
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: ed54d6d8-d00f-11e1-986c-000c29cc1a4c
    description: ! "VMware SHG v4.x & v5.x - NCN04 - Ensure that the â\x80\x9CForged
      Transmitsâ\x80\x9D policy is set to â\x80\x9Creject.â\x80\x9D"
    modifier: allow
    expression: !ruby/object:MiqExpression
    exp:

```

```

      FIND:
        checkall:
          =:
            value: 'false'
            field: Host.lans-forged_transmits
        search:
          IS NOT NULL:
            value: ''
            field: Host.lans-name
        context_type:
      towhat: Host
      file_mtime:
      guid: ed54d6d8-d00f-11e1-986c-000c29cc1a4c
      filename:
      applies_to_exp:
      miq_policy_id: 8
      notes: ! "VMware SHG v4.x & v5.x - NCN04 - Ensure that the â\x80\x9CForged Transmitsâ\x80\x9D
        policy is set to â\x80\x9Creject.â\x80\x9D R1"
- MiqPolicy:
  name: d7ed01f4-d00e-11e1-986c-000c29cc1a4c
  description: ! "VMware SHG v4.x & v5.x - NCN05 -Ensure that the â\x80\x9CPromiscuous
    Modeâ\x80\x9D policy is set to â\x80\x9Creject.â\x80\x9D R1"
  expression: !ruby/object:MiqExpression
  exp:
    =:
      field: Host-vmm_product
      value: ESXi
  context_type:
  towhat: Host
  guid: d7ed01f4-d00e-11e1-986c-000c29cc1a4c
  created_by: admin
  updated_by: admin
  notes: ! "VMware SHG v4.x & v5.x - NCN05 -Ensure that the â\x80\x9CPromiscuous
    Modeâ\x80\x9D policy is set to â\x80\x9Creject.â\x80\x9D R1"
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: abb1772c-d00f-11e1-986c-000c29cc1a4c
    description: ! "VMware SHG v4.x & v5.x - NCN05 -Ensure that the â\x80\x9CPromiscuous
      Modeâ\x80\x9D policy is set to â\x80\x9Creject.â\x80\x9D R1"
    modifier: allow

```

```

    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkall:
            =:
              field: Host.lans-allow_promiscuous
              value: 'false'
          search:
            IS NOT NULL:
              field: Host.lans-name
              value: ''
          context_type:
        towhat: Host
        file_mtime:
        guid: abb1772c-d00f-11e1-986c-000c29cc1a4c
        filename:
        applies_to_exp:
        miq_policy_id: 9
        notes: ! "VMware SHG v4.x & v5.x - NCN05 -Ensure that the \x80\x9CPromiscuous
          Mode\x80\x9D policy is set to \x80\x9Creject.\x80\x9D R1"
- MiqPolicy:
  name: 86c84f3a-d005-11e1-986c-000c29cc1a4c
  description: VMware SHG v4.x & v5.x - NCN10 - Ensure that port groups are configured
    with a clear network label
  expression: !ruby/object:MiqExpression
    exp:
      =:
        field: Host-vmm_product
        value: ESXi
    context_type:
  towhat: Host
  guid: 86c84f3a-d005-11e1-986c-000c29cc1a4c
  created_by: admin
  updated_by: admin
  notes: VMware SHG v4.x & v5.x - NCN10 - Ensure that port groups are configured
    with a clear network label R1
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: elc666a0-d006-11e1-986c-000c29cc1a4c
    description: VMware SHG v4.x & v5.x - NCN10 - Ensure that port groups are configured
      with a clear network label

```

```

    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        or:
          - FIND:
              checkcount:
                =:
                  field: <count>
                  value: '0'
              search:
                IS NULL:
                  field: Host.lans-name
                  value: ''
          - FIND:
              checkcount:
                =:
                  value: '0'
                  field: <count>
              search:
                IS EMPTY:
                  value: ''
                  field: Host.lans-name
          context_type:
        towhat: Host
        file_mtime:
        guid: e1c666a0-d006-11e1-986c-000c29cc1a4c
        filename:
        applies_to_exp:
        miq_policy_id: 11
        notes: VMware SHG v4.x & v5.x - NCN10 - Ensure that port groups are configured
              with a clear network label R1
- MiqPolicy:
    name: cee396f8-clf0-11e1-ae68-000c29cc1a4c
    description: VMware SHG v4.x & v5.x - VMX02 - Prevent other users from spying
      on administrator remote consoles.
    expression: !ruby/object:MiqExpression
      exp:
        =:
          value: VMware
          field: Vm-vendor
      context_type:
    towhat: Vm
    guid: cee396f8-clf0-11e1-ae68-000c29cc1a4c
    created_by: admin
    updated_by: admin
    notes: VMware SHG v4.x & v5.x - VMX02 - Prevent other users from spying on administrator
      remote consoles.
    active: true
    mode: compliance
    MiqPolicyContent:
      - qualifier: failure
        failure_sequence: 1
    MiqEvent:
      name: vm_compliance_check
      description: VM Compliance Check
      guid: 816a598a-f57d-11de-a41a-005056ba0614
      event_type: Default
      definition:
        default:

```



```

    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
- name: 71089c6c-clf1-11e1-ae68-000c29cc1a4c
  description: VMware SHG v4.x & v5.x - VMX02 - Prevent other users from spying
    on administrator remote consoles.
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          =:
            value: '1'
            field: Vm.advanced_settings-value
        search:
          =:
            value: RemoteDisplay.maxConnections
            field: Vm.advanced_settings-name
        context_type:
      towhat: Vm
      file_mtime:
      guid: 71089c6c-clf1-11e1-ae68-000c29cc1a4c
      filename:
      applies_to_exp:
      miq_policy_id: 2
      notes: VMware SHG v4.x & v5.x - VMX02 - Prevent other users from spying on administrator
        remote consoles. R1
- MiqPolicy:
  name: 1d60a788-clf3-11e1-ae68-000c29cc1a4c
  description: VMware SHG v4.x & v5.x - VMX11 Prevent unauthorized removal, connection
    and modification of devices
  expression: !ruby/object:MiqExpression
    exp:
      and:
      - =:
          field: Vm-vendor
          value: VMware
      - STARTS WITH:
          value: '5'
          field: Vm.host-vmm_version
      context_type:
    towhat: Vm
    guid: 1d60a788-clf3-11e1-ae68-000c29cc1a4c
    created_by: admin
    updated_by: admin
    notes: VMware SHG v4.x & v5.x - VMX11 Prevent unauthorized removal, connection
      and modification of devices
    active: true
    mode: compliance
    MiqPolicyContent:
      - qualifier: failure
        failure_sequence: 1
    MiqEvent:
      name: vm_compliance_check

```

```

description: VM Compliance Check
guid: 816a598a-f57d-11de-a41a-005056ba0614
event_type: Default
definition:
  default:
  enabled:
MiqAction:
  name: compliance_failed
  description: Mark as Non-Compliant
  guid: ba452d94-f586-11de-8ebc-0050568a07c7
  action_type: default
  options: {}
Condition:
- name: 728e7050-c1f3-11e1-ae68-000c29cc1a4c
  description: VMware SHG v5.x - VMX11 Prevent unauthorized removal, connection
    and modification of devices
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          =:
            value: 'true'
            field: Vm.advanced_settings-value
        search:
          =:
            value: isolation.device.connectable.disable
            field: Vm.advanced_settings-name
        context_type:
towhat: Vm
file_mtime:
guid: 728e7050-c1f3-11e1-ae68-000c29cc1a4c
filename:
applies_to_exp: !ruby/object:MiqExpression
  exp:
    STARTS WITH:
      field: Vm.host-vmm_version
      value: '5'
    context_type:
miq_policy_id: 12
notes: VMware SHG v5.x - VMX11 Prevent unauthorized removal, connection and
  modification of devices R1
- name: aaa64a08-d7d8-11e1-b3e5-000c2999f7f1
  description: VMware SHG v4.x - VMX11 Prevent unauthorized removal, connection
    and modification of devices
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      and:
      - FIND:
        checkany:
          =:
            value: 'true'
            field: Vm.advanced_settings-value
        search:
          =:
            value: isolation.device.connectable.disable
            field: Vm.advanced_settings-name
      - FIND:

```

```

      checkany:
        =:
          field: Vm.advanced_settings-value
          value: 'true'
      search:
        =:
          field: Vm.advanced_settings-name
          value: isolation.device.edit.disable
      context_type:
      towhat: Vm
      file_mtime:
      guid: aaa64a08-d7d8-11e1-b3e5-000c2999f7f1
      filename:
      applies_to_exp: !ruby/object:MiqExpression
      exp:
        STARTS WITH:
          value: '4'
          field: Vm.host-vmm_version
      context_type:
      miq_policy_id: 12
      notes: VMware SHG v4.x - VMX11 Prevent unauthorized removal, connection and
        modification of devices R1
- MiqPolicy:
  name: 769b4b1e-clf8-11e1-ae68-000c29cc1a4c
  description: VMware SHG v4.x & v5.x - VMX30 - Disable remote operations within
    the guest.
  expression: !ruby/object:MiqExpression
  exp:
    =:
      value: VMware
      field: Vm-vendor
  context_type:
  towhat: Vm
  guid: 769b4b1e-clf8-11e1-ae68-000c29cc1a4c
  created_by: admin
  updated_by: admin
  notes: VMware SHG v4.x & v5.x - VMX30 - Disable remote operations within the guest.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: vm_compliance_check
    description: VM Compliance Check
    guid: 816a598a-f57d-11de-a41a-005056ba0614
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: 8b7f39d2-clf8-11e1-ae68-000c29cc1a4c
    description: VMware SHG v4.x - VMX30 - Disable remote operations within the

```

```

    guest.
  modifier: allow
  expression: !ruby/object:MiqExpression
  exp:
    FIND:
      checkany:
        =:
          field: Vm.advanced_settings-value
          value: 'false'
      search:
        =:
          field: Vm.advanced_settings-name
          value: guest.commands.enabled
    context_type:
  towhat: Vm
  file_mtime:
  guid: 8b7f39d2-c1f8-11e1-ae68-000c29cc1a4c
  filename:
  applies_to_exp: !ruby/object:MiqExpression
  exp:
    STARTS WITH:
      value: '4'
      field: Vm.host-vmm_version
    context_type:
  miq_policy_id: 16
  notes: VMware SHG v4.x - VMX30 - Disable remote operations within the guest.
  R1
- MiqPolicy:
  name: e99a4c3e-d00b-11e1-986c-000c29cc1a4c
  description: VMware SHG v4x. & v5.x - NCN11 - Ensure that all vSwitches have a
    clear network label.
  expression: !ruby/object:MiqExpression
  exp:
    =:
      value: ESXi
      field: Host-vmm_product
    context_type:
  towhat: Host
  guid: e99a4c3e-d00b-11e1-986c-000c29cc1a4c
  created_by: admin
  updated_by: admin
  notes: VMware SHG v4x. & v5.x - NCN11 - Ensure that all vSwitches have a clear
    network label. R1
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant

```

```

    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: 5ca4abca-d00c-11e1-986c-000c29cc1a4c
    description: VMware SHG v4x. & v5.x - NCN11 - Ensure that all vSwitches have
      a clear network label.
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        or:
        - FIND:
            checkall:
              IS NOT NULL:
                value: ''
                field: Host.hardware.ports-device_name
            search:
              =:
                value: ethernet
                field: Host.hardware.ports-device_type
        - FIND:
            checkall:
              IS NOT EMPTY:
                field: Host.hardware.ports-device_name
                value: ''
            search:
              =:
                field: Host.hardware.ports-device_type
                value: ethernet
            context_type:
            towhat: Host
            file_mtime:
            guid: 5ca4abca-d00c-11e1-986c-000c29cc1a4c
            filename:
            applies_to_exp:
            miq_policy_id: 10
            notes: VMware SHG v4x. & v5.x - NCN11 - Ensure that all vSwitches have a clear
              network label. R1
  - MiqPolicy:
      name: d4640a18-e15d-11e1-acfa-005056b25af6
      description: powervm
      expression:
      towhat: Vm
      guid: d4640a18-e15d-11e1-acfa-005056b25af6
      created_by: admin
      updated_by: admin
      notes:
      active: true
      mode: control
      MiqPolicyContent:
      - qualifier: success
        success_sequence: 1
      MiqEvent:
        name: vm_start
        description: VM Power On
        guid: 404b4630-21a8-11e2-b47a-0050568b19a3
        event_type: Default
        definition:
        default:

```

```

    enabled:
  MiqAction:
    name: b0138b70-e15d-11e1-8744-005056b25af6
    description: powerVM
    guid: b0138b70-e15d-11e1-8744-005056b25af6
    action_type: custom_automation
    options:
      :ae_message: create
      :ae_request: powerVM
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_poweroff
    description: VM Power Off
    guid: 48beeadc-ae7c-11e1-a76f-005056b25af6
    event_type: Default
    definition:
      default:
        enabled:
  MiqAction:
    name: b0138b70-e15d-11e1-8744-005056b25af6
    description: powerVM
    guid: b0138b70-e15d-11e1-8744-005056b25af6
    action_type: custom_automation
    options:
      :ae_message: create
      :ae_request: powerVM
Condition: []

```

### 3.18.2 Profiles.yaml

Link: [Profiles.yaml](#)

Source:

```

---
- MiqPolicySet:
  name: 612b936c-3d2d-11df-a7e9-005056a40709
  description: ! 'ACTIVE - Analysis: Manage VMs'
  set_type: MiqPolicySet
  guid: 612b936c-3d2d-11df-a7e9-005056a40709
  read_only:
  set_data:
    :notes: ! '1)Create a new Tag Category called Operations (Show in EVM Console
      and Single Value)

      2)Create the following Tags under this new Operations Category (analysis_failed,
      analysis_required, analysis_success)

      3)Create Global Filters for VMs for Analysis Failed and Analysis Required
      to easily find tagged VMs.

      4)Set up a Schedule to run as desired that will process the VMs that currently
      match the Global Filter. Ex: Analyze all VMs that are tagged with "Analysis
      Required".

```

```

mode: control
owner_type:
owner_id:
MiqPolicy:
- name: 07cea762-3d1b-11df-a7e9-005056a40709
  description: ! 'Tag: VM if Analysis not successful'
  expression:
  towhat: Vm
  guid: 07cea762-3d1b-11df-a7e9-005056a40709
  created_by: admin
  updated_by: admin
  notes:
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_scan_abort
      description: VM Analysis Failure
      guid: 4c48a6fa-37c0-11df-b567-005056a40709
      event_type: Default
      definition:
      default:
      enabled:
    MiqAction:
      name: fc7f2dde-3d22-11df-a7e9-005056a40709
      description: Tag VM that Fails Analysis
      guid: fc7f2dde-3d22-11df-a7e9-005056a40709
      action_type: tag
      options:
        :variables:
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>

```

```

      - :value: ''
        :oid: ''
        :var_type: <None>
      :tags:
      - /managed/operations/analysis_failed
    Condition: []
  - name: 0ce6cf38-3d2d-11df-a7e9-005056a40709
    description: ! 'Tag: VM on Successful Analysis'
    expression:
    towhat: Vm
    guid: 0ce6cf38-3d2d-11df-a7e9-005056a40709
    created_by: admin
    updated_by: admin
    notes:
    active: true
    mode: control
    MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_scan_complete
      description: VM Analysis Complete
      guid: f7b8361e-1139-11e1-9333-005056af009e
      event_type: Default
      definition:
      default:
      enabled:
    MiqAction:
      name: cd2f3222-3d2c-11df-a7e9-005056a40709
      description: Tag VM after Successful Analysis
      guid: cd2f3222-3d2c-11df-a7e9-005056a40709
      action_type: tag
      options:
      :tags:
      - /managed/operations/analysis_success
    Condition: []
  - name: b968f0a0-3d2e-11df-a7e9-005056a40709
    description: ! 'Tag: VM that Requires Analysis'
    expression:
    towhat: Vm
    guid: b968f0a0-3d2e-11df-a7e9-005056a40709
    created_by: admin
    updated_by: admin
    notes:
    active: true
    mode: control
    MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_start
      description: VM Power On
      guid: 404b4630-21a8-11e2-b47a-0050568b19a3
      event_type: Default
      definition:
      default:
      enabled:
    MiqAction:
      name: a4ccd026-3d2e-11df-a7e9-005056a40709

```



```

    description: Tag VM that Requires Analysis
    guid: a4ccd026-3d2e-11df-a7e9-005056a40709
    action_type: tag
    options:
      :tags:
        - /managed/operations/analysis_required
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_create
    description: VM Create Complete
    guid: 4c0b4f12-37c0-11df-b567-005056a40709
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: a4ccd026-3d2e-11df-a7e9-005056a40709
    description: Tag VM that Requires Analysis
    guid: a4ccd026-3d2e-11df-a7e9-005056a40709
    action_type: tag
    options:
      :tags:
        - /managed/operations/analysis_required
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_reset
    description: VM Reset
    guid: 4c1b8a3a-37c0-11df-b567-005056a40709
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: a4ccd026-3d2e-11df-a7e9-005056a40709
    description: Tag VM that Requires Analysis
    guid: a4ccd026-3d2e-11df-a7e9-005056a40709
    action_type: tag
    options:
      :tags:
        - /managed/operations/analysis_required
  Condition: []
- name: ! 'Do Not Analyze '
  description: ! 'Analysis: Prevent Analysis of Selected VMs'
  expression:
  towhat: Vm
  guid: 3a7959c0-2866-11de-af2a-0050568026c2
  created_by:
  updated_by: admin
  notes: ! 'This policies prevents analysis ofany vm that is tagged as Do Not
    Analyze '
  active: true
  mode: control
  MiqPolicyContent:
    - qualifier: success
      success_sequence: 1
      failure_synchronous: true
  MiqEvent:

```

```

    name: request_vm_scan
    description: VM Analysis Request
    guid: e3292c46-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
    MiqAction:
      name: prevent
      description: Prevent current event from proceeding
      guid: d885a118-519b-11e0-8d82-005056af0000
      action_type: default
      options: {}
    Condition:
  - name: Do Not Analyze
    description: VM classified as DO_NOT_ANALYZE
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        CONTAINS:
          tag: Vm.managed-exclusions
          value: do_not_analyze
        context_type:
      towhat: Vm
      file_mtime:
      guid: 39ff4444-08e2-11de-829f-005056a164b2
      filename:
      applies_to_exp:
      miq_policy_id: 10000000000001
      notes:
- MiqPolicySet:
  name: 74de8372-bbd6-11e1-a4a4-005056b25af6
  description: ACTIVE - Prevent PowerOn of Quarantined VMs
  set_type: MiqPolicySet
  guid: 74de8372-bbd6-11e1-a4a4-005056b25af6
  read_only:
  set_data:
  mode: control
  owner_type:
  owner_id:
  MiqPolicy:
  - name: f4f0e916-bbd5-11e1-a4a4-005056b25af6
    description: Prevent PowerOn of Quarantined VM
    expression:
    towhat: Vm
    guid: f4f0e916-bbd5-11e1-a4a4-005056b25af6
    created_by: admin
    updated_by: admin
    notes:
    active: true
    mode: control
    MiqPolicyContent:
    - qualifier: success
      success_sequence: 1
    MiqEvent:
      name: request_vm_start
      description: VM Power On Request
      guid: 48b02c4a-ae7c-11e1-a76f-005056b25af6
      event_type: Default

```

```

    definition:
    default:
    enabled:
  MiqAction:
    name: vm_stop
    description: Stop Virtual Machine
    guid: 37f2da3e-21a8-11e2-b47a-0050568b19a3
    action_type: default
    options: {}
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_start
    description: VM Power On
    guid: 404b4630-21a8-11e2-b47a-0050568b19a3
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: vm_stop
    description: Stop Virtual Machine
    guid: 37f2da3e-21a8-11e2-b47a-0050568b19a3
    action_type: default
    options: {}
  Condition:
- name: 1cbc27da-bbd6-11e1-ac0c-005056b25af6
  description: VM Tagged as Do Not PowerOn
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      CONTAINS:
        tag: Vm.managed-exclusions
        value: do_not_power_on
      context_type:
  towhat: Vm
  file_mtime:
  guid: 1cbc27da-bbd6-11e1-ac0c-005056b25af6
  filename:
  applies_to_exp:
  miq_policy_id:
  notes:
- MiqPolicySet:
  name: 3a78daca-99da-11e1-a4bf-005056b057a8
  description: ! 'ACTIVE - Snapshot Management: Max of 2'
  set_type: MiqPolicySet
  guid: 3a78daca-99da-11e1-a4bf-005056b057a8
  read_only:
  set_data:
  mode: control
  owner_type:
  owner_id:
  MiqPolicy:
- name: cf87e7fc-99d8-11e1-a4bf-005056b057a8
  description: ! 'Snapshots: limit to max of 2'
  expression:
  towhat: Vm
  guid: cf87e7fc-99d8-11e1-a4bf-005056b057a8
  created_by: admin

```

```

updated_by: admin
notes: This policy prevents a vm from starting if there are more than 2 snapshots.
      If this number is exceeded, the vm is not allowed to start and the vm annotations
      are updated in the VC
active: true
mode: control
MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_start
    description: VM Power On
    guid: 404b4630-21a8-11e2-b47a-0050568b19a3
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: vm_stop
    description: Stop Virtual Machine
    guid: 37f2da3e-21a8-11e2-b47a-0050568b19a3
    action_type: default
    options: {}
- qualifier: success
  success_sequence: 2
  MiqEvent:
    name: vm_start
    description: VM Power On
    guid: 404b4630-21a8-11e2-b47a-0050568b19a3
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: 8d6ebd90-99d9-11e1-a4bf-005056b057a8
    description: ! 'VM Attribute: Max Snapshots'
    guid: 8d6ebd90-99d9-11e1-a4bf-005056b057a8
    action_type: set_custom_attribute
    options:
      :value: Snapshot Limit Exceeded
      :attribute: EVM Policy
Condition:
- name: 9db4783a-99d8-11e1-a4bf-005056b057a8
  description: Snapshot Count >=3
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      ! '>=':
        count: Vm.snapshots
        value: '3'
    context_type:
  towhat: Vm
  file_mtime:
  guid: 9db4783a-99d8-11e1-a4bf-005056b057a8
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000079
  notes: This condition checks to see if 3 or more snapshots exist
- MiqPolicySet:

```

```

name: 98eea278-8b9f-11e0-b8fc-005056a40e59
description: ACTIVE - VMs in DMZ NIC Check
set_type: MiqPolicySet
guid: 98eea278-8b9f-11e0-b8fc-005056a40e59
read_only:
set_data:
  :notes: This Policy Profile will check VM Network Adapter count and if > 1 will
    Stop the VM. This will happen after VM Analysis is Complete or when the VM
    is Powered On.
mode: control
owner_type:
owner_id:
MiqPolicy:
- name: 69fbd202-8ba3-11e0-b8fc-005056a40e59
  description: DMZ - Shutdown VM after Analysis if it has more than 1 NIC
  expression: !ruby/object:MiqExpression
    exp:
      =:
        value: 'on'
        field: Vm-power_state
    context_type:
  towhat: Vm
  guid: 69fbd202-8ba3-11e0-b8fc-005056a40e59
  created_by: admin
  updated_by: admin
  notes:
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_scan_complete
      description: VM Analysis Complete
      guid: f7b8361e-1139-11e1-9333-005056af009e
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: vm_shutdown_guest
      description: Shutdown Virtual Machine Guest OS
      guid: 26b84380-bbd5-11de-aaab-0050568a2c6a
      action_type: default
      options: {}
  - qualifier: success
    success_sequence: 2
    MiqEvent:
      name: vm_scan_complete
      description: VM Analysis Complete
      guid: f7b8361e-1139-11e1-9333-005056af009e
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: evm_event
      description: Show EVM Event on Timeline
      guid: 16b1810c-44e8-11e0-acda-005056a40e59

```

```

      action_type: default
      options: {}
    Condition:
    - name: efcf3702-8b9e-11e0-b8fc-005056a40e59
      description: DMZ - VM has more than 1 NIC
      modifier: allow
      expression: !ruby/object:MiqExpression
        exp:
          ! '>':
            count: Vm.hardware.nics
            value: '1'
          context_type:
            towhat: Vm
            file_mtime:
            guid: efcf3702-8b9e-11e0-b8fc-005056a40e59
            filename:
            applies_to_exp:
            miq_policy_id: 10000000000077
            notes:
    - name: 0de66508-8b9f-11e0-b8fc-005056a40e59
      description: DMZ - Shutdown VM after Starting if it has more than 1 NIC
      expression:
      towhat: Vm
      guid: 0de66508-8b9f-11e0-b8fc-005056a40e59
      created_by: admin
      updated_by: admin
      notes:
      active: true
      mode: control
      MiqPolicyContent:
      - qualifier: success
        success_sequence: 1
      MiqEvent:
        name: vm_start
        description: VM Power On
        guid: 404b4630-21a8-11e2-b47a-0050568b19a3
        event_type: Default
        definition:
          default:
          enabled:
      MiqAction:
        name: vm_stop
        description: Stop Virtual Machine
        guid: 37f2da3e-21a8-11e2-b47a-0050568b19a3
        action_type: default
        options: {}
      - qualifier: success
        success_sequence: 2
      MiqEvent:
        name: vm_start
        description: VM Power On
        guid: 404b4630-21a8-11e2-b47a-0050568b19a3
        event_type: Default
        definition:
          default:
          enabled:
      MiqAction:
        name: evm_event
        description: Show EVM Event on Timeline

```

```

    guid: 16b1810c-44e8-11e0-acda-005056a40e59
    action_type: default
    options: {}
- qualifier: success
  success_sequence: 3
  MiqEvent:
    name: vm_start
    description: VM Power On
    guid: 404b4630-21a8-11e2-b47a-0050568b19a3
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: d91bbabc-b0be-11e1-b0dc-005056b057a8
    description: ! 'VM Attribute: Allowed NIC Count Exceeded'
    guid: d91bbabc-b0be-11e1-b0dc-005056b057a8
    action_type: set_custom_attribute
    options:
      :attribute: EVM Policy
      :value: Allowed NIC Limit Exceeded
  Condition:
- name: efcf3702-8b9e-11e0-b8fc-005056a40e59
  description: DMZ - VM has more than 1 NIC
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      ! '>':
        count: Vm.hardware.nics
        value: '1'
    context_type:
    towhat: Vm
    file_mtime:
    guid: efcf3702-8b9e-11e0-b8fc-005056a40e59
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000077
    notes:
- MiqPolicySet:
  name: 820849ce-a7fb-11e0-abed-005056af0000
  description: ! 'Analysis: Do Not Analyze Active VDI VMs'
  set_type: MiqPolicySet
  guid: 820849ce-a7fb-11e0-abed-005056af0000
  read_only:
  set_data:
    :notes: This policy profile checks to see if a VDI vm is being actively used
      by a user. If a user is currently connected to the session, it will prevent
      the vm from being analyzed
  mode: control
  owner_type:
  owner_id:
  MiqPolicy:
- name: 1c4c7772-a7fb-11e0-abed-005056af0000
  description: Do Not Analyze Active VDI VMs
  expression:
  towhat: Vm
  guid: 1c4c7772-a7fb-11e0-abed-005056af0000
  created_by: admin
  updated_by: admin

```

```

notes: This policy prevents analysis of a vm that has an active user session
active: true
mode: control
MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_scan_start
    description: VM Analysis Start
    guid: 057b9baa-519c-11e0-8d82-005056af0000
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: prevent
    description: Prevent current event from proceeding
    guid: d885a118-519b-11e0-8d82-005056af0000
    action_type: default
    options: {}
  Condition:
- name: 0a50f750-a7fb-11e0-abad-005056af0000
  description: VM has an active session
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      =:
        value: 'true'
        field: Vm-has_active_vdi_session
    context_type:
  towhat: Vm
  file_mtime:
  guid: 0a50f750-a7fb-11e0-abad-005056af0000
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000007
  notes:
- MiqPolicySet:
  name: 43e76af6-3f8e-11e0-aaa0-00505688000a
  description: ! 'Analysis: Exclude Specially Tagged VMs'
  set_type: MiqPolicySet
  guid: 43e76af6-3f8e-11e0-aaa0-00505688000a
  read_only:
  set_data:
    :notes: Prevents the analysis of vms tagged as do not analyze
  mode: control
  owner_type:
  owner_id:
  MiqPolicy:
- name: ! 'Do Not Analyze '
  description: ! 'Analysis: Prevent Analysis of Selected VMs'
  expression:
  towhat: Vm
  guid: 3a7959c0-2866-11de-af2a-0050568026c2
  created_by:
  updated_by: admin
  notes: ! 'This policies prevents analysis ofany vm that is tagged as Do Not
    Analyze '
  active: true

```



```

mode: control
MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  failure_synchronous: true
  MiqEvent:
    name: request_vm_scan
    description: VM Analysis Request
    guid: e3292c46-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: prevent
    description: Prevent current event from proceeding
    guid: d885a118-519b-11e0-8d82-005056af0000
    action_type: default
    options: {}
  Condition:
- name: Do Not Analyze
  description: VM classified as DO_NOT_ANALYZE
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      CONTAINS:
        tag: Vm.managed-exclusions
        value: do_not_analyze
      context_type:
      towhat: Vm
      file_mtime:
      guid: 39ff4444-08e2-11de-829f-005056a164b2
      filename:
      applies_to_exp:
      miq_policy_id: 10000000000001
      notes:
- MiqPolicySet:
  name: 3872a0e8-50bc-11e0-880e-00505688000a
  description: ! 'Analysis: On VM Reconfiguration'
  set_type: MiqPolicySet
  guid: 3872a0e8-50bc-11e0-880e-00505688000a
  read_only:
  set_data:
    :notes: Triggers a VM analysis when a VM is reconfigured
  mode: control
  owner_type:
  owner_id:
  MiqPolicy:
- name: 2f2a1alc-4806-11df-badc-005056a7121f
  description: ! 'Analysis: VM Reconfiguration'
  expression:
  towhat: Vm
  guid: 2f2a1alc-4806-11df-badc-005056a7121f
  created_by: admin
  updated_by: admin
  notes: Performs an analysis on any vm that has been reconfigured
  active: true
  mode: control
  MiqPolicyContent:

```

```

- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_reconfigure
    description: VM Settings Change
    guid: 07367e62-449a-11de-bd4f-005056a83e5d
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: vm_analyze
    description: Initiate SmartState Analysis for VM
    guid: 5cbe1082-ce35-11de-a117-005056b0503e
    action_type: default
    options: {}
  Condition: []
- MiqPolicySet:
  name: 079d2408-44ef-11e0-99a6-00505688000a
  description: ! 'Analysis: VDI Login'
  set_type: MiqPolicySet
  guid: 079d2408-44ef-11e0-99a6-00505688000a
  read_only:
  set_data:
    :notes: This policy profile automatically analyzes a VDI session when a user
      logs in to it.
  mode: control
  owner_type:
  owner_id:
  MiqPolicy:
  - name: 782068f8-44ee-11e0-99a6-00505688000a
    description: ! 'Analysis: VDI Login'
    expression:
    towhat: Vm
    guid: 782068f8-44ee-11e0-99a6-00505688000a
    created_by: admin
    updated_by: admin
    notes: This policy triggers an analysis of a VDI session when a user logs in
      to that session
    active: true
    mode: control
    MiqPolicyContent:
    - qualifier: success
      success_sequence: 1
      MiqEvent:
        name: vm_vdi_login_session
        description: VDI Login Session
        guid: 15fc3cce-448a-11e0-9ad1-00505688000a
        event_type: Default
        definition:
          default:
          enabled:
      MiqAction:
        name: vm_analyze
        description: Initiate SmartState Analysis for VM
        guid: 5cbe1082-ce35-11de-a117-005056b0503e
        action_type: default
        options: {}
      Condition: []

```

```

- MiqPolicySet:
  name: aa699b96-de34-11e1-9088-005056af009e
  description: Collect VDI User Information
  set_type: MiqPolicySet
  guid: aa699b96-de34-11e1-9088-005056af009e
  read_only:
  set_data:
  mode: control
  owner_type:
  owner_id:
  MiqPolicy:
  - name: 57189108-d1d3-11e1-9ede-005056af009e
    description: Record Last RDP User
    expression:
    towhat: Vm
    guid: 57189108-d1d3-11e1-9ede-005056af009e
    created_by: admin
    updated_by: admin
    notes: ! 'When a user logs on to the VM through an RDP session, the file c:\rdp_login\ ↵
      rdp.log
      is automatically created by the logon script.

```

A analysis profile should be set to retrieve this file and its content.

This policy will automatically raise an automate event so the content of the file can be parsed and elements set as custom attributes of the VM '

```

active: true
mode: control
MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_scan_complete
    description: VM Analysis Complete
    guid: f7b8361e-1139-11e1-9333-005056af009e
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: raise_automation_event
    description: Raise Automation Event
    guid: e7da3b7a-1139-11e1-9333-005056af009e
    action_type: default
    options: {}
  Condition:
  - name: 5a4c3456-de30-11e1-9088-005056af009e
    description: Check for files starting with rep
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkcount:
            ! '>=':
              field: <count>
              value: '1'
          search:

```

```

      INCLUDES:
        field: Vm.filesystems-name
        value: rdp
      context_type:
    towhat: Vm
    file_mtime:
    guid: 5a4c3456-de30-11e1-9088-005056af009e
    filename:
    applies_to_exp:
    miq_policy_id: 4
    notes:
- name: d658fe5c-de2c-11e1-9088-005056af009e
  description: Collect Logged on User Info
  expression:
  towhat: Vm
  guid: d658fe5c-de2c-11e1-9088-005056af009e
  created_by: admin
  updated_by: admin
  notes:
  active: true
  mode: control
  MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_scan_complete
    description: VM Analysis Complete
    guid: f7b8361e-1139-11e1-9333-005056af009e
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: raise_automation_event
    description: Raise Automation Event
    guid: e7da3b7a-1139-11e1-9333-005056af009e
    action_type: default
    options: {}
  Condition:
- name: ab61c97a-de2e-11e1-9088-005056af009e
  description: Check files starting with nb
  modifier: allow
  expression: !ruby/object:MiqExpression
  exp:
    FIND:
      checkcount:
        ! '>=':
          value: '1'
          field: <count>
      search:
        INCLUDES:
          value: nb
          field: Vm.filesystems-name
        context_type:
      towhat: Vm
      file_mtime:
      guid: ab61c97a-de2e-11e1-9088-005056af009e
      filename:
      applies_to_exp:

```

```

    miq_policy_id: 5
    notes:
- MiqPolicySet:
  name: e4bcd3de-2480-11e2-b7d5-005056b25af6
  description: ! 'Compliance Hosts: November 2012'
  set_type: MiqPolicySet
  guid: e4bcd3de-2480-11e2-b7d5-005056b25af6
  read_only:
  set_data:
  mode: control
  owner_type:
  owner_id:
  MiqPolicy:
- name: de683aa6-fedf-11de-83dd-005056ba5e76
  description: Network - Mac Changes not Allowed
  expression:
  towhat: Host
  guid: de683aa6-fedf-11de-83dd-005056ba5e76
  created_by: admin
  updated_by: admin
  notes: This policy checks that MAC changes are not allowed on vSwitches and
    vLans.
  active: true
  mode: compliance
  MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
- name: 0a6eb332-fee0-11de-83dd-005056ba5e76
  description: Mac Changes Disabled in vSwitches
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      not:
        CONTAINS:
          value: 'false'
          field: Host.switches-mac_changes
  towhat: Host
  file_mtime:
  guid: 0a6eb332-fee0-11de-83dd-005056ba5e76
  filename:
  applies_to_exp:
  miq_policy_id: 100000000000028
  notes: This condition verifies that MAC changes are not allowed on vSwitches.
- name: 3ed9fb4a-fee0-11de-83dd-005056ba5e76

```

```

description: Mac Changes Disabled in vLans
modifier: allow
expression: !ruby/object:MiqExpression
  exp:
    not:
      CONTAINS:
        value: 'false'
        field: Host.lans-mac_changes
towhat: Host
file_mtime:
guid: 3ed9fb4a-fee0-11de-83dd-005056ba5e76
filename:
applies_to_exp:
miq_policy_id: 10000000000028
notes: This condition verifies that MAC changes are not allowed on vLans.
- name: 61b355f2-fee1-11de-83dd-005056ba5e76
description: Network - Forged Transmits Must Be Disabled
expression:
towhat: Host
guid: 61b355f2-fee1-11de-83dd-005056ba5e76
created_by: admin
updated_by: admin
notes: This policy insures that forged transmits are disabled on both vLans
      and vSwitches.
active: true
mode: compliance
MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
Condition:
- name: f246e3e0-fee1-11de-83dd-005056ba5e76
description: Forged Transmits Disabled in vLan
modifier: allow
expression: !ruby/object:MiqExpression
  exp:
    not:
      CONTAINS:
        value: 'false'
        field: Host.lans-forged_transmits
towhat: Host
file_mtime:
guid: f246e3e0-fee1-11de-83dd-005056ba5e76
filename:
applies_to_exp:
miq_policy_id: 10000000000022

```

```

    notes: This condition verifies that forged transmits are disabled on vlans.
  - name: a3ac5774-fee1-11de-83dd-005056ba5e76
    description: Forged Transmits Disabled in vSwitch
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        not:
          CONTAINS:
            value: 'false'
            field: Host.switches-forged_transmits
    towhat: Host
    file_mtime:
    guid: a3ac5774-fee1-11de-83dd-005056ba5e76
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000022
    notes: This condition verifies that forged transmits are disabled on vSwitches.
- MiqPolicySet:
  name: 587352f0-fb88-11de-a067-005056ba0614
  description: ! 'Compliance: Hosts'
  set_type: MiqPolicySet
  guid: 587352f0-fb88-11de-a067-005056ba0614
  read_only:
  set_data:
    :notes: This policy profile validates that an ESX host meets the standard defined
      in VMWare's security hardening documentation
  mode: pr
  owner_type:
  owner_id:
  MiqPolicy:
  - name: eb84f288-fa39-11de-83ca-005056ba0614
    description: Protect Root File System Filling /home
    expression:
    towhat: Host
    guid: eb84f288-fa39-11de-83ca-005056ba0614
    created_by: admin
    updated_by: admin
    notes: This policy verifies that the /home directory is mounted on a different
      partition than the root filesystem.
    active: true
    mode: compliance
    MiqPolicyContent:
    - qualifier: failure
      failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
      default:
      enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:

```

```

- name: 62447a1a-fa3a-11de-83ca-005056ba0614
  description: Protect Root File System Filling /home
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^[^\#]*\./home
            field: Host.filesystems-contents
          search:
            =:
              value: /etc/fstab
              field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: 62447a1a-fa3a-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 10000000000019
        notes: This condition verifies that the file /etc/fstab has an uncommented
              line that references the directory /home.
- name: 04db603c-fa3a-11de-83ca-005056ba0614
  description: Firewall - Outgoing Security Level
  expression:
  towhat: Host
  guid: 04db603c-fa3a-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that only a defined set of outgoing TCP and UDP
        Ports are open.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
- name: f0afd7d6-fa3a-11de-83ca-005056ba0614
  description: Valid Outgoing TCP Ports
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      LIMITED TO:
        value: '902,427,443,27000,27010'
        field: Host-enabled_tcp_outbound_ports

```



```

    towhat: Host
    file_mtime:
    guid: f0afd7d6-fa3a-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000020
    notes: This condition verifies that the only open outgoing TCP ports are ↵
           427,443,902,27000,
           and 27010.
- name: 1778fb28-fa44-11de-83ca-005056ba0614
  description: Valid Outgoing UDP Ports
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      LIMITED TO:
        value: '427,123,902'
        field: Host-enabled_udp_outbound_ports
    towhat: Host
    file_mtime:
    guid: 1778fb28-fa44-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000020
    notes: This condition verifies that the only open outgoing UDP ports are 123,427,
           and 902.
- name: af2d74ea-fa39-11de-83ca-005056ba0614
  description: Firewall - Incoming Security Level
  expression:
    towhat: Host
    guid: af2d74ea-fa39-11de-83ca-005056ba0614
    created_by: admin
    updated_by: admin
    notes: This policy verifies that only a defined set of incoming TCP and UDP
           Ports are open.
    active: true
    mode: compliance
    MiqPolicyContent:
      - qualifier: failure
        failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
    Condition:
      - name: b4a0843a-fa43-11de-83ca-005056ba0614
        description: Valid Incoming UDP Ports
        modifier: allow
        expression: !ruby/object:MiqExpression
          exp:

```

```

    LIMITED TO:
      value: '427'
      field: Host-enabled_udp_inbound_ports
  towhat: Host
  file_mtime:
  guid: b4a0843a-fa43-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 100000000000021
  notes: This condition verifies that the only open incoming UDP port is 427.
- name: 03529e9e-f961-11de-9e9d-0050568a07c7
  description: Valid Incoming TCP Ports
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      LIMITED TO:
        value: '902,80,443,427,5989,22,5988'
        field: Host-enabled_tcp_inbound_ports
  towhat: Host
  file_mtime:
  guid: 03529e9e-f961-11de-9e9d-0050568a07c7
  filename:
  applies_to_exp:
  miq_policy_id: 100000000000021
  notes: This condition verifies that the only open incoming TCP ports are ←
        22,80,427,443,902,5988,and
        5989.
- name: 61b355f2-fee1-11de-83dd-005056ba5e76
  description: Network - Forged Transmits Must Be Disabled
  expression:
  towhat: Host
  guid: 61b355f2-fee1-11de-83dd-005056ba5e76
  created_by: admin
  updated_by: admin
  notes: This policy insures that forged transmits are disabled on both vLans
        and vSwitches.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: f246e3e0-fee1-11de-83dd-005056ba5e76
    description: Forged Transmits Disabled in vLan
    modifier: allow

```

```

    expression: !ruby/object:MiqExpression
      exp:
        not:
          CONTAINS:
            value: 'false'
            field: Host.lans-forged_transmits
        towhat: Host
        file_mtime:
        guid: f246e3e0-fee1-11de-83dd-005056ba5e76
        filename:
        applies_to_exp:
        miq_policy_id: 10000000000022
        notes: This condition verifies that forged transmits are disabled on vlans.
- name: a3ac5774-fee1-11de-83dd-005056ba5e76
  description: Forged Transmits Disabled in vSwitch
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      not:
        CONTAINS:
          value: 'false'
          field: Host.switches-forged_transmits
      towhat: Host
      file_mtime:
      guid: a3ac5774-fee1-11de-83dd-005056ba5e76
      filename:
      applies_to_exp:
      miq_policy_id: 10000000000022
      notes: This condition verifies that forged transmits are disabled on vSwitches.
- name: 8d4a7bee-fa56-11de-83ca-005056ba0614
  description: Timekeeping - Minimum of 3 NTP Servers defined in step-tickers
  expression:
    towhat: Host
    guid: 8d4a7bee-fa56-11de-83ca-005056ba0614
    created_by: admin
    updated_by: admin
    notes: This policy verifies that a minimum of 3 servers are defined in the NTP
      step-tickers configuration.
    active: true
    mode: compliance
    MiqPolicyContent:
      - qualifier: failure
        failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
- name: 0806448a-fa57-11de-83ca-005056ba0614

```

```

description: Verify 3 NTP Servers Defined in step-tickers File
modifier: allow
expression: !ruby/object:MiqExpression
  exp:
    FIND:
      checkany:
        RUBY:
          value: ! "count = 0\ncontext.each_line { |line| ←
            #
            Break up the input by lines\n  count += 1 if line =~ /^[^#]*server\\s+[0-9 ←
              A-Za-z]+/
            \  # Increment Count if line matches our regular expression\n}\nreturn
              true if count >= 3\nreturn false\n"
          field: Host.filesystems-contents
        search:
          =:
            value: /etc/ntp/step-tickers
            field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: 0806448a-fa57-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 100000000000023
        notes: This condition checks the file /etc/ntp/step-tickers and verifies that
          a minimum of three ntp servers are defined.
- name: ab373d88-fa4a-11de-83ca-005056ba0614
description: Settings - Display Logs on Different Terminals
expression:
towhat: Host
guid: ab373d88-fa4a-11de-83ca-005056ba0614
created_by: admin
updated_by: admin
notes: This policy verifies that critical, error, and warning level log messages
  are directed to distinct terminals.
active: true
mode: compliance
MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
- name: f383ec6c-fa4a-11de-83ca-005056ba0614
description: Verify Different Logs Displayed on Different Terminals
modifier: allow
expression: !ruby/object:MiqExpression

```

```

exp:
  and:
    - FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^\s*\*\.crit\s+\/dev\/tty
            field: Host.filesystems-contents
          search:
            =:
              value: /etc/syslog.conf
              field: Host.filesystems-name
    - FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^\s*\*\.err\s+\/dev\/tty
            field: Host.filesystems-contents
          search:
            =:
              value: /etc/syslog.conf
              field: Host.filesystems-name
    - FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^\s*\*\.warning\s+\/dev\/tty
            field: Host.filesystems-contents
          search:
            =:
              value: /etc/syslog.conf
              field: Host.filesystems-name
  towhat: Host
  file_mtime:
  guid: f383ec6c-fa4a-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 100000000000024
  notes: This condition checks the file /etc/syslog.conf has three separate
    parameters defined for critical, error, and warning level log messages.
    These parameters specify the tty will display the specified log messages.
- name: 498f5330-fa4b-11de-83ca-005056ba0614
  description: Settings - Remote syslog Logging
  expression:
  towhat: Host
  guid: 498f5330-fa4b-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that syslog is configured to utilize a remote server.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
    default:
    enabled:

```

```

    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
  - name: ee09af6e-fa4b-11de-83ca-005056ba0614
    description: Verify syslog Utilizes a Remote Host
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:
              value: /^[^#*]\s*.*@/
              field: Host.filesystems-contents
          search:
            =:
              value: /etc/syslog.conf
              field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: ee09af6e-fa4b-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 100000000000025
        notes: This condition checks the file /etc/syslog.conf and verifies the existence
              of the @ parameter, which is used to specify the use of a remote server.
  - name: eb0151ea-fa47-11de-83ca-005056ba0614
    description: Root Login on console should be Disabled
    expression:
      towhat: Host
      guid: eb0151ea-fa47-11de-83ca-005056ba0614
      created_by: admin
      updated_by: admin
      notes: This policy verifies that the root account cannot directly login via
            the console.
      active: true
      mode: compliance
    MiqPolicyContent:
      - qualifier: failure
        failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
  - name: 571e6e76-fa48-11de-83ca-005056ba0614

```

```

description: File /etc/securetty should be empty
modifier: allow
expression: !ruby/object:MiqExpression
  exp:
    FIND:
      checkall:
        =:
          value: '0'
          field: Host.filesystems-size
      search:
        =:
          value: /etc/securetty
          field: Host.filesystems-name
  towhat: Host
  file_mtime:
  guid: 571e6e76-fa48-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 100000000000026
  notes: This condition checks the file /etc/securetty and verifies that it's
    empty by checking for a 0KB file size.
- name: e4c93c82-fa3a-11de-83ca-005056ba0614
  description: Permissions - /etc/grub.conf
  expression:
  towhat: Host
  guid: e4c93c82-fa3a-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that editing the server's boot process requires
    root level authority.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: d2adb400-fa3b-11de-83ca-005056ba0614
    description: Permissions - /etc/grub.conf
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        and:
          - FIND:
              checkany:
                =:

```

```

        value: '0600'
        field: Host.filesystems-permissions
      search:
        =:
        value: /etc/grub.conf
        field: Host.filesystems-name
    - FIND:
      checkany:
        =:
        value: root
        field: Host.filesystems-owner
      search:
        =:
        value: /etc/grub.conf
        field: Host.filesystems-name
    towhat: Host
    file_mtime:
    guid: d2adb400-fa3b-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000027
    notes: This condition verifies that the file /etc/grub.conf's permissions
           are set to 0600 and is owned by root.
  - name: de683aa6-fedf-11de-83dd-005056ba5e76
    description: Network - Mac Changes not Allowed
    expression:
    towhat: Host
    guid: de683aa6-fedf-11de-83dd-005056ba5e76
    created_by: admin
    updated_by: admin
    notes: This policy checks that MAC changes are not allowed on vSwitches and
           vLans.
    active: true
    mode: compliance
    MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
      default:
      enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
    Condition:
  - name: 0a6eb332-fee0-11de-83dd-005056ba5e76
    description: Mac Changes Disabled in vSwitches
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
      not:
      CONTAINS:

```



```

        value: 'false'
        field: Host.switches-mac_changes
    towhat: Host
    file_mtime:
    guid: 0a6eb332-fee0-11de-83dd-005056ba5e76
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000028
    notes: This condition verifies that MAC changes are not allowed on vSwitches.
- name: 3ed9fb4a-fee0-11de-83dd-005056ba5e76
  description: Mac Changes Disabled in vLans
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      not:
        CONTAINS:
          value: 'false'
          field: Host.lans-mac_changes
    towhat: Host
    file_mtime:
    guid: 3ed9fb4a-fee0-11de-83dd-005056ba5e76
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000028
    notes: This condition verifies that MAC changes are not allowed on vLans.
- name: 7cc14778-fe0f-11de-83dd-005056ba5e76
  description: Network - Promiscuous Mode Setting Not Disabled
  expression:
  towhat: Host
  guid: 7cc14778-fe0f-11de-83dd-005056ba5e76
  created_by: admin
  updated_by: admin
  notes: Check the Host VLAN setting for Promiscuous Mode which should be disabled.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
- name: 2045b314-fe58-11de-83dd-005056ba5e76
  description: Check Host vSwitch - Promiscuous Mode Must Not Be Enable
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      not:

```

```

      CONTAINS:
        value: 'true'
        field: Host.switches-allow_promiscuous
    towhat: Host
    file_mtime:
    guid: 2045b314-fe58-11de-83dd-005056ba5e76
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000029
    notes: This condition verifies that vSwitches do not allow Promiscuous mode
           via inheritance.
- name: 80e5ff5e-fe16-11de-83dd-005056ba5e76
  description: Check Host Port - Promiscuous Mode Must Not Be Enabled
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      not:
        CONTAINS:
          value: 'true'
          field: Host.lans-computed_allow_promiscuous
    towhat: Host
    file_mtime:
    guid: 80e5ff5e-fe16-11de-83dd-005056ba5e76
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000029
    notes: This condition verifies that vLans do not allow Promiscuous mode via
           inheritance.
- name: a8e0ef7c-fa48-11de-83ca-005056ba0614
  description: Use sudo aliases
  expression:
    towhat: Host
  guid: a8e0ef7c-fa48-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that user aliases are enabled in the configuration
        of the sudo command.
  active: true
  mode: compliance
  MiqPolicyContent:
    - qualifier: failure
      failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
    - name: 99496ebc-fa49-11de-83ca-005056ba0614
      description: Aliases are being used for sudo authorization

```

```

    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:
              value: ^\s*User_Alias
              field: Host.filesystems-contents
          search:
            =:
              value: /etc/sudoers
              field: Host.filesystems-name
    towhat: Host
    file_mtime:
    guid: 99496ebc-fa49-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000030
    notes: This condition checks the file /etc/sudoers and verifies that the parameter
           "User_Alias" is defined.
- name: 4ed279b2-fa55-11de-83ca-005056ba0614
  description: Timekeeping - NTP Service Running
  expression:
  towhat: Host
  guid: 4ed279b2-fa55-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that the NTP servers is configured to automatically
        start.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
- name: 9a08d21e-fa55-11de-83ca-005056ba0614
  description: Verify NTP is Running
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          INCLUDES:
            value: '3'
            field: Host.host_services-enable_run_levels

```

```

      search:
        =:
          value: ntpd
          field: Host.host_services-name
    towhat: Host
    file_mtime:
    guid: 9a08d21e-fa55-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000031
    notes: This condition verifies that the run level of the service ntpd is set
      to three.
- name: a6c2a51e-fa57-11de-83ca-005056ba0614
  description: Timekeeping - Minimum of 3 NTP Servers Defined in ntp.conf
  expression:
  towhat: Host
  guid: a6c2a51e-fa57-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that a minimum of 3 servers are defined in the NTP
    configuration.
  active: true
  mode: compliance
  MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
- name: 03c821bc-fa58-11de-83ca-005056ba0614
  description: Verify 3 NTP Servers Defined in ntp.conf
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          RUBY:
            value: ! "count = 0\ncontext.each_line { |line|
              #
              Break up the input by lines\n  count += 1 if line =~ /^[^#]*server\\s+[0-9
              A-Za-z]+/
              \  # Increment Count if line matches our regular expression\n}\nreturn
              true if count >= 3\nreturn false"
            field: Host.filesystems-contents
          search:
            =:
              value: /etc/ntp.conf

```

```

        field: Host.filesystems-name
    towhat: Host
    file_mtime:
    guid: 03c821bc-fa58-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000032
    notes: This condition checks the file /etc/ntp.conf and verifies that a minimum
      of three ntp servers are defined.
- name: c4396f3a-fa55-11de-83ca-005056ba0614
  description: Timekeeping - Minimum of 3 NTP Servers Defined in hosts
  expression:
  towhat: Host
  guid: c4396f3a-fa55-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that a minimum of 3 NTP servers are defined in the
    local hosts file.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
- name: 2698c39c-fa56-11de-83ca-005056ba0614
  description: Verify 3 NTP Servers Defined in hosts File
  modifier: allow
  expression: !ruby/object:MiqExpression
  exp:
    FIND:
      checkany:
      RUBY:
        value: ! "count = 0\ncontext.each_line { |line| ↵
          #
          Break up the input by lines\n  count += 1 if line =~ /^[^#]*NTP/i
          \ # Increment Count if line matches our regular expression\n}\nreturn
          true if count >= 3\nreturn false\n"
        field: Host.filesystems-contents
      search:
        =:
          value: /etc/hosts
          field: Host.filesystems-name
    towhat: Host
    file_mtime:
    guid: 2698c39c-fa56-11de-83ca-005056ba0614

```

```

    filename:
    applies_to_exp:
    miq_policy_id: 100000000000033
    notes: ! 'This conditions checks the file /etc/hosts and veries that there
      are at least 3 uncommented lines that reference ntp servers. The included
      expression can be modified to match the appropriate values for the ntp servers
      for your environment.
  ,
- name: 3819638c-fa57-11de-83ca-005056ba0614
  description: Timekeeping - Drift Enabled
  expression:
  towhat: Host
  guid: 3819638c-fa57-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that NTP's driftfile support is enabled.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
- name: 71fae5da-fa57-11de-83ca-005056ba0614
  description: Verify NTP Uses a Driftfile
  modifier: allow
  expression: !ruby/object:MiqExpression
  exp:
    FIND:
      checkany:
        REGULAR EXPRESSION MATCHES:
          value: ^\s*driftfile\s+\/var\/lib\/ntp\/drift
          field: Host.filesystems-contents
      search:
        =:
          value: /etc/ntp.conf
          field: Host.filesystems-name
  towhat: Host
  file_mtime:
  guid: 71fae5da-fa57-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 100000000000034
  notes: This condition checks the file /etc/ntp.conf and verifies that the
    driftfile parameter exists.

```

```

- name: ebc02cea-fa57-11de-83ca-005056ba0614
  description: Time Keeping - Restrict Access for Machines without Loopback
  expression:
  towhat: Host
  guid: ebc02cea-fa57-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that only non-loopback machines can access the NTP
        service.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
      default:
      enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
  - name: ddc26260-fa58-11de-83ca-005056ba0614
    description: Access Restricted for Machines without Loopback
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:
              value: ^\s*restrict\s+default\s+kod\s+nomodify\s+notrap
              field: Host.filesystems-contents
          search:
            =:
              value: /etc/ntp.conf
              field: Host.filesystems-name
    towhat: Host
    file_mtime:
    guid: ddc26260-fa58-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000035
    notes: This condition checks the file /etc/ntp.conf and verifies that the
          line "restrict default kod nomodify notrap" exists.
- name: ccadf9fa-fa56-11de-83ca-005056ba0614
  description: Time Keeping - NTP Configured to Use Loopback Adapter
  expression:
  towhat: Host
  guid: ccadf9fa-fa56-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that NTP performs all name resolutions via a loopback

```

```

    network.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: 2b9bb8b2-fa57-11de-83ca-005056ba0614
    description: NTP Configured to Use Loopback Adapter
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:
              value: ^\s*restrict\s+127\.0\.0\.1
              field: Host.filesystems-contents
          search:
            =:
              value: /etc/ntp.conf
              field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: 2b9bb8b2-fa57-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 100000000000036
        notes: This condition checks the file /etc/ntp.conf and verifies that the
              restrict parameter's value is set to 127.0.0.1.
  - name: 4614d62e-fa52-11de-83ca-005056ba0614
    description: Settings - vmkwarning Compress Option
    expression:
    towhat: Host
    guid: 4614d62e-fa52-11de-83ca-005056ba0614
    created_by: admin
    updated_by: admin
    notes: This policy verifies that the vmkwarning log is compressed by default.
    active: true
    mode: compliance
    MiqPolicyContent:
    - qualifier: failure
      failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check

```



```

    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
- name: a51cbaba-fa52-11de-83ca-005056ba0614
  description: Verify Compression Enabled in vmkwarning
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: \s+compress
            field: Host.filesystems-contents
        search:
          =:
            value: /etc/logrotate.d/vmkwarning
            field: Host.filesystems-name
  towhat: Host
  file_mtime:
  guid: a51cbaba-fa52-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 100000000000037
  notes: This condition checks the file /etc/logrotate.d/vmkwarning and verifies
        that the option compress is enabled.
- name: 6353b57e-fa53-11de-83ca-005056ba0614
  description: Settings - vmksummary Compress Option
  expression:
  towhat: Host
  guid: 6353b57e-fa53-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that the vmksummary log is compressed by default.
  active: true
  mode: compliance
  MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7

```

```

    action_type: default
    options: {}
  Condition:
  - name: 510f7286-fa53-11de-83ca-005056ba0614
    description: Verify Compression Enabled in vmksummary
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:
              value: \s+compress
              field: Host.filesystems-contents
            search:
              =:
                value: /etc/logrotate.d/vmksummary
                field: Host.filesystems-name
          towhat: Host
          file_mtime:
          guid: 510f7286-fa53-11de-83ca-005056ba0614
          filename:
          applies_to_exp:
          miq_policy_id: 100000000000038
          notes: This condition checks the file /etc/logrotate.d/vmksummary and verifies
            that the option compress is enabled.
  - name: 0864fae6-fa54-11de-83ca-005056ba0614
    description: Settings - vmkernel Compress Option
    expression:
    towhat: Host
    guid: 0864fae6-fa54-11de-83ca-005056ba0614
    created_by: admin
    updated_by: admin
    notes: This policy verifies that the vmkernel log is compressed by default.
    active: true
    mode: compliance
    MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
      default:
      enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
  - name: fe7378be-fa53-11de-83ca-005056ba0614
    description: Verify Compression Enabled in vmkernel
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:

```

```

      checkany:
        REGULAR EXPRESSION MATCHES:
          value: \s+compress
          field: Host.filesystems-contents
      search:
        =:
          value: /etc/logrotate.d/vmkernel
          field: Host.filesystems-name
    towhat: Host
    file_mtime:
    guid: fe7378be-fa53-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000039
    notes: This condition checks the file /etc/logrotate.d/vmkernel and verifies
           that the option compress is enabled.
- name: 6576a074-fa48-11de-83ca-005056ba0614
  description: Settings - /etc/sudoers
  expression:
  towhat: Host
  guid: 6576a074-fa48-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that sudo is configured to use syslog for logging.
  active: true
  mode: compliance
  MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
- name: adel86c6-fa48-11de-83ca-005056ba0614
  description: Verify sudo is Logging via syslog
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^\s*Defaults\s+syslog\|=
            field: Host.filesystems-contents
        search:
          =:
            value: /etc/sudoers
            field: Host.filesystems-name
    towhat: Host

```

```

    file_mtime:
    guid: adel86c6-fa48-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000040
    notes: This condition check the file /etc/sudoers and verifies that the parameter
           "Defaults syslog=" exists.
- name: c340f524-fa3e-11de-83ca-005056ba0614
  description: Settings - /etc/grub.conf
  expression:
  towhat: Host
  guid: c340f524-fa3e-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that a password is required in order to edit the
        server's boot process.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
      default:
      enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
  - name: 1f18225a-fa3f-11de-83ca-005056ba0614
    description: Verify /etc/grub.conf Settings
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:
              value: ^\s*password\s\-\md5
              field: Host.filesystems-contents
          search:
            =:
              value: /etc/grub.conf
              field: Host.filesystems-name
    towhat: Host
    file_mtime:
    guid: 1f18225a-fa3f-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000041
    notes: This condition check the file /etc/grub.conf and verifies that the
          parameter "password --md5" exists.
- name: c63b0560-fa45-11de-83ca-005056ba0614

```

```

description: Root Login via SSH should be Disabled
expression:
towhat: Host
guid: c63b0560-fa45-11de-83ca-005056ba0614
created_by: admin
updated_by: admin
notes: This policy verifies that the root account cannot login to the host via
      SSH.
active: true
mode: compliance
MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
Condition:
- name: 4435b6d6-fa46-11de-83ca-005056ba0614
  description: PermitRootLogin = no in sshd_config file
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^\s*PermitRootLogin\s+no
            field: Host.filesystems-contents
        search:
          =:
            value: /etc/ssh/sshd_config
            field: Host.filesystems-name
  towhat: Host
  file_mtime:
  guid: 4435b6d6-fa46-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000042
  notes: This condition checks the file /etc/ssh/sshd_config and verifies that
        the PermitRootLogin parameter's value is set to no.
- name: 5ce6be9a-fa4c-11de-83ca-005056ba0614
  description: Require users to enter own password - no ROOTPW entry
  expression:
  towhat: Host
  guid: 5ce6be9a-fa4c-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that when the sudo command is used, each user is
        prompted for their password and not the root password.

```

```

active: true
mode: compliance
MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
- name: a791b882-fa4c-11de-83ca-005056ba0614
  description: ROOTPW does not exist in sudoers file
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION DOES NOT MATCH:
            value: /^[^#]*ROOTPW/i
            field: Host.filesystems-contents
        search:
          =:
            value: /etc/sudoers
            field: Host.filesystems-name
    towhat: Host
    file_mtime:
    guid: a791b882-fa4c-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000043
    notes: This condition check the file /etc/sudoers and verifies that it does
      not contain the word ROOTPW on an uncommented line.
- name: a128d356-fa36-11de-83ca-005056ba0614
  description: Protect Root File System Filling /tmp
  expression:
  towhat: Host
  guid: a128d356-fa36-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that the /tmp directory is mounted on a different
    partition than the root filesystem.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check

```

```

    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
- name: 267dd9de-fa37-11de-83ca-005056ba0614
  description: Protect Root File System Filling /tmp
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^[^\#]*\tmp
            field: Host.filesystems-contents
        search:
          =:
            value: /etc/fstab
            field: Host.filesystems-name
  towhat: Host
  file_mtime:
  guid: 267dd9de-fa37-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 100000000000044
  notes: This condition verifies that the file /etc/fstab has an uncommented
        line that references the directory /tmp.
- name: 7ea7db8c-fa46-11de-83ca-005056ba0614
  description: Permissions - /etc/snmp/snmpd.conf
  expression:
  towhat: Host
  guid: 7ea7db8c-fa46-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy ensures that access to SNMP configuration parameters are
        limited to the root user.
  active: true
  mode: compliance
  MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant

```

```

    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
Condition:
- name: ebb24a50-fa46-11de-83ca-005056ba0614
  description: Permissions - /etc/snmp/snmpd.conf
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      and:
        - FIND:
            checkany:
              =:
                value: '0700'
                field: Host.filesystems-permissions
            search:
              =:
                value: /etc/snmp/snmpd.conf
                field: Host.filesystems-name
        - FIND:
            checkany:
              =:
                value: root
                field: Host.filesystems-owner
            search:
              =:
                value: /etc/snmp/snmpd.conf
                field: Host.filesystems-name
  towhat: Host
  file_mtime:
  guid: ebb24a50-fa46-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000045
  notes: This condition verifies that the permissions of /etc/snmp/snmpd.conf
    are 0700 and is owned by root.
- name: 40b796dc-fa50-11de-83ca-005056ba0614
  description: Password Expiration Warning Default
  expression:
  towhat: Host
  guid: 40b796dc-fa50-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies the default setting for password expiration warning.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed

```



```

    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: 0e842bde-fa51-11de-83ca-005056ba0614
    description: Password Expiration Warning Default >= 7days
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:
              value: ^\s*PASS_WARN_AGE\s+([7-9]|[1-9][0-9]+)
              field: Host.filesystems-contents
            search:
              =:
                value: /etc/login.defs
                field: Host.filesystems-name
          towhat: Host
          file_mtime:
            guid: 0e842bde-fa51-11de-83ca-005056ba0614
            filename:
              applies_to_exp:
                miq_policy_id: 10000000000046
                notes: This condition checks the file /etc/login.defs and verifies that PASS_WARN_AGE
                  parameter's value is set to 7 or greater.
          - name: 2f9fad14-fa4e-11de-83ca-005056ba0614
            description: Password Aging - Default Maximum
            expression:
              towhat: Host
              guid: 2f9fad14-fa4e-11de-83ca-005056ba0614
              created_by: admin
              updated_by: admin
              notes: This policy validates the ESX host's maximum password age configuration.
              active: true
              mode: compliance
              MiqPolicyContent:
                - qualifier: failure
                  failure_sequence: 1
                MiqEvent:
                  name: host_compliance_check
                  description: Host Compliance Check
                  guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
                  event_type: Default
                  definition:
                    default:
                      enabled:
                MiqAction:
                  name: compliance_failed
                  description: Mark as Non-Compliant
                  guid: ba452d94-f586-11de-8ebc-0050568a07c7
                  action_type: default
                  options: {}
            Condition:
            - name: a4a0e740-fa4e-11de-83ca-005056ba0614
              description: Default Maximum Password Age <= 90days
              modifier: allow
              expression: !ruby/object:MiqExpression

```

```

    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^\s*PASS_MAX_DAYS\s+([0-9]|[1-8][0-9]|90)
            field: Host.filesystems-contents
          search:
            =:
              value: /etc/login.defs
              field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: a4a0e740-fa4e-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 10000000000047
        notes: This condition checks the file /etc/login.defs and verifies that the
              PASS_MAX_DAYS parameter's value is 90 days or greater.
- name: 79548666-fa51-11de-83ca-005056ba0614
  description: Limit vmkwarning Size
  expression:
  towhat: Host
  guid: 79548666-fa51-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy checks the vmkwarning log is limited to a specified size.
  active: true
  mode: compliance
  MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
- name: 14d35e46-fa52-11de-83ca-005056ba0614
  description: vmkwarning Log Size <= 4096KB
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^\s*size\s+(409[0-6]|40[0-8][0-9]|[123][0-9]{3}|\d{1,3})k
            field: Host.filesystems-contents
          search:
            =:
              value: /etc/logrotate.d/vmkwarning

```

```

        field: Host.filesystems-name
    towhat: Host
    file_mtime:
    guid: 14d35e46-fa52-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000048
    notes: This condition verifies that the file /etc/logrotate.d/vmkernel warning is
           configured to limit the associated log to 4096KB.
- name: c79821fa-fa53-11de-83ca-005056ba0614
  description: Limit vmkernel Size
  expression:
  towhat: Host
  guid: c79821fa-fa53-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy checks the vmkernel log is limited to a specified size.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
- name: be9722e0-fa53-11de-83ca-005056ba0614
  description: vmkernel Log Size <= 4096KB
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^\s*size\s+(409[0-6]|40[0-8][0-9]|123[0-9]{3}|\d{1,3})k
            field: Host.filesystems-contents
          search:
            =:
              value: /etc/logrotate.d/vmkernel
              field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: be9722e0-fa53-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 100000000000049
        notes: This condition verifies that the file /etc/logrotate.d/vmkernel is
               configured to limit the associated log to 4096KB.

```

```

- name: 8cecc84c-fa46-11de-83ca-005056ba0614
  description: Limit su Access to root Account
  expression:
  towhat: Host
  guid: 8cecc84c-fa46-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy validates that only members of the group wheel can access
    the su command.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
      default:
      enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
  - name: 63b243fc-fa47-11de-83ca-005056ba0614
    description: Only members of wheel group can execute su command
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:
              value: ^\s*auth\s+required\s+.*pam_wheel\.so\s+use_uid
              field: Host.filesystems-contents
          search:
            =:
              value: /etc/pam.d/su
              field: Host.filesystems-name
    towhat: Host
    file_mtime:
    guid: 63b243fc-fa47-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000050
    notes: This condition validates that the file /etc/pam.d/su contains a variation
      of the string "auth required pam_wheel.so use_uid".
  - name: 2cd1b736-fa52-11de-83ca-005056ba0614
    description: Limit Software and Services Running in Service Console
    expression:
    towhat: Host
    guid: 2cd1b736-fa52-11de-83ca-005056ba0614
    created_by: admin
    updated_by: admin
    notes: This policy validates that only an approved list of services are enabled

```

```

    at boot time on an ESX host.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: c4c80bfa-fa55-11de-83ca-005056ba0614
    description: Default Services Running in Service Console
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        LIMITED TO:
          value: crond, firewall, gpm, ipmi, irqbalance, mgmt-vmware, microcode_ctl,
            mptctlnode, network, ntpd, pegasus, portmap, random, rawdevices, sshd,
            syslog, vmware, vmware-autostart, vmware-late, vmware-vmkauthd, vmware-vpxa,
            vmware-webAccess, wsman, xinetd
          field: Host-enabled_run_level_3_services
    towhat: Host
    file_mtime:
    guid: c4c80bfa-fa55-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000051
    notes: This conditions validates that a defined list of services are enabled
      with the ESX host is booted with networking support (run level 3). This
      list includes the generic services included in ESX. Additional hardware
      specific services can be added to the expression.
  - name: edaf1082-fa54-11de-83ca-005056ba0614
    description: Firewall - Outgoing NTP Port
    expression:
    towhat: Host
    guid: edaf1082-fa54-11de-83ca-005056ba0614
    created_by: admin
    updated_by: admin
    notes: This policy validates that the Firewall is configured properly for NTP
      support.
    active: true
    mode: compliance
    MiqPolicyContent:
    - qualifier: failure
      failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check

```

```

    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
- name: 1cb7f0ba-fa55-11de-83ca-005056ba0614
  description: Valid NTP Outgoing UDP Port
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      INCLUDES ANY:
        value: '123'
        field: Host-enabled_udp_outbound_ports
  towhat: Host
  file_mtime:
  guid: 1cb7f0ba-fa55-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000052
  notes: This condition verifies that the outgoing UDP port required by NTP
        (port 123) is open.
- name: 0f2cc826-fa4b-11de-83ca-005056ba0614
  description: Directory Service Used for Authentication for sudo
  expression:
  towhat: Host
  guid: 0f2cc826-fa4b-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that sudo is configured to use a directory for user
        authentication.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
- name: 684b2a60-fa4b-11de-83ca-005056ba0614
  description: Directory Service used for sudo authentication

```

```

    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:
              value: ^\s*auth\s+required\s+.*pam_stack\.so\s+service=system-auth
              field: Host.filesystems-contents
          search:
            =:
              value: /etc/pam.d/sudo
              field: Host.filesystems-name
    towhat: Host
    file_mtime:
    guid: 684b2a60-fa4b-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000053
    notes: ! 'This condition verifies that the line "auth required pam_stack.so
      service=system-auth" exists in /etc/pam.d/sudo. '
- name: 4b188948-fa45-11de-83ca-005056ba0614
  description: Settings - SNMP Read Only Access
  expression:
  towhat: Host
  guid: 4b188948-fa45-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that SNMP is configured to only allow read-only
    access.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
- name: e328c720-fa45-11de-83ca-005056ba0614
  description: SNMP Configured for Read-only Access
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      and:
      - FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:
              value: ^\s*rocommunity

```

```

        field: Host.filesystems-contents
      search:
        =:
          value: /etc/snmp/snmpd.conf
          field: Host.filesystems-name
    - FIND:
      checkany:
        REGULAR EXPRESSION DOES NOT MATCH:
          value: ^\s*rwcommunity
          field: Host.filesystems-contents
      search:
        =:
          value: /etc/snmp/snmpd.conf
          field: Host.filesystems-name
    towhat: Host
    file_mtime:
    guid: e328c720-fa45-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000054
    notes: This condition checks the file /etc/snmp/snmpd.conf and verifies that
           the rocommunity parameter is defined and the rwcommunity parameter is not.
  - name: 854d45aa-fa3a-11de-83ca-005056ba0614
    description: Protect Root File System Filling /var/log
    expression:
    towhat: Host
    guid: 854d45aa-fa3a-11de-83ca-005056ba0614
    created_by: admin
    updated_by: admin
    notes: This policy verifies that the /var/log directory is mounted on a different
           partition than the root filesystem.
    active: true
    mode: compliance
    MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
    Condition:
  - name: a84173e2-fa3a-11de-83ca-005056ba0614
    description: Protect Root File System Filling /var/log
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            REGULAR EXPRESSION MATCHES:

```



```

        value: ^[^\#]*\var\log
        field: Host.filesystems-contents
    search:
    =:
        value: /etc/fstab
        field: Host.filesystems-name
    towhat: Host
    file_mtime:
    guid: a84173e2-fa3a-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000055
    notes: This condition verifies that the file /etc/fstab has an uncommented
           line that references the directory /var/log.
- name: fc63df74-fa52-11de-83ca-005056ba0614
  description: Limit vmksummary Size
  expression:
  towhat: Host
  guid: fc63df74-fa52-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy checks the vmksummary log is limited to a specified size.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
- name: def33840-fa52-11de-83ca-005056ba0614
  description: vmksummary Log Size <= 4096KB
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^\s*size\s+(409[0-6]|40[0-8][0-9]|[123][0-9]{3}|\d{1,3})k
            field: Host.filesystems-contents
          search:
            =:
              value: /etc/logrotate.d/vmksummary
              field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: def33840-fa52-11de-83ca-005056ba0614

```

```

    filename:
    applies_to_exp:
    miq_policy_id: 100000000000056
    notes: This condition verifies that the file /etc/logrotate.d/vmksummary is
           configured to limit the associated log to 4096KB.
- name: 305e6832-fa51-11de-83ca-005056ba0614
  description: Password Complexity - Minimum Length
  expression:
  towhat: Host
  guid: 305e6832-fa51-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies the minimum password length.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: compliance_failed
      description: Mark as Non-Compliant
      guid: ba452d94-f586-11de-8ebc-0050568a07c7
      action_type: default
      options: {}
  Condition:
- name: c0ba559e-fa51-11de-83ca-005056ba0614
  description: Minimum Password Length >= 8
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^\s*PASS_MIN_LEN\s+([8-9]|[1-9][0-9]+)
            field: Host.filesystems-contents
          search:
            =:
              value: /etc/login.defs
              field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: c0ba559e-fa51-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 100000000000057
        notes: This condition checks the file /etc/login.defs and verifies that the
              PASS_MIN_LEN parameter's value is 8 or greater.
- name: e6f082ba-fa4c-11de-83ca-005056ba0614
  description: Password checking enabled for sudo
  expression:
  towhat: Host

```

```

guid: e6f082ba-fa4c-11de-83ca-005056ba0614
created_by: admin
updated_by: admin
notes: This policy verifies that password checking is enabled for sudo.
active: true
mode: compliance
MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
Condition:
- name: 3d2074e2-fa4d-11de-83ca-005056ba0614
  description: NOPASSWD does not exist in sudoers file
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION DOES NOT MATCH:
            value: /^[^#]*NOPASSWD/i
            field: Host.filesystems-contents
        search:
          =:
            value: /etc/sudoers
            field: Host.filesystems-name
    towhat: Host
    file_mtime:
  guid: 3d2074e2-fa4d-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 100000000000058
  notes: This condition check the file /etc/sudoers and verifies that it does
    not contain the word NOPASSWORD on an uncommented line.
- name: 32b26f2c-fa4f-11de-83ca-005056ba0614
  description: Password Aging - Default Minimum
  expression:
  towhat: Host
  guid: 32b26f2c-fa4f-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy validates the ESX host's minimum password age configuration.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1

```

```

MiqEvent:
  name: host_compliance_check
  description: Host Compliance Check
  guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
  event_type: Default
  definition:
    default:
    enabled:
MiqAction:
  name: compliance_failed
  description: Mark as Non-Compliant
  guid: ba452d94-f586-11de-8ebc-0050568a07c7
  action_type: default
  options: {}
Condition:
- name: 79d39ad4-fa4f-11de-83ca-005056ba0614
  description: Default Minimum Password Age >= 0
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^\s*PASS_MIN_DAYS\s+\d+
            field: Host.filesystems-contents
          search:
            =:
              value: /etc/login.defs
              field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: 79d39ad4-fa4f-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 100000000000059
        notes: This condition checks the file /etc/login.defs and verifies that the
          PASS_MIN_DAYS parameter's value is greater than or equal to 0 days.
- MiqPolicySet:
  name: 97c27462-1592-11df-b613-0050568a1ed6
  description: ! 'Compliance: VM'
  set_type: MiqPolicySet
  guid: 97c27462-1592-11df-b613-0050568a1ed6
  read_only:
  set_data:
    :notes: This policy profile validates that a vm meets the standard defined in
      VMWare's security hardening documentation
  mode: control
  owner_type:
  owner_id:
  MiqPolicy:
- name: 2d6bfc2c-fa3b-11de-83ca-005056ba0614
  description: Limit Log Size
  expression:
  towhat: Vm
  guid: 2d6bfc2c-fa3b-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes:
  active: true

```

```

mode: compliance
MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: vm_compliance_check
    description: VM Compliance Check
    guid: 816a598a-f57d-11de-a41a-005056ba0614
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
Condition:
- name: 8b9cf076-fa3b-11de-83ca-005056ba0614
  description: Log Size Limit <= 100KB
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkall:
          <=:
            value: '100000'
            field: Vm.advanced_settings-value
        search:
          =:
            value: log.rotateSize
            field: Vm.advanced_settings-name
    towhat: Vm
    file_mtime:
    guid: 8b9cf076-fa3b-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000061
    notes:
- name: flaf8b44-fa3b-11de-83ca-005056ba0614
  description: Limit Number of Log Files
  expression:
  towhat: Vm
  guid: flaf8b44-fa3b-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes:
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: vm_compliance_check
      description: VM Compliance Check
      guid: 816a598a-f57d-11de-a41a-005056ba0614
      event_type: Default
      definition:

```

```

    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: f2ad72ac-fa3d-11de-83ca-005056ba0614
    description: Number of Log Files to Keep <= 10
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkall:
            <=:
              value: '10'
              field: Vm.advanced_settings-value
          search:
            =:
              value: log.keepOld
              field: Vm.advanced_settings-name
        towhat: Vm
        file_mtime:
        guid: f2ad72ac-fa3d-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 100000000000060
        notes:
  - MiqPolicySet:
    name: 17fa069a-480b-11df-badc-005056a7121f
    description: ! 'Demo: CPU Reservation'
    set_type: MiqPolicySet
    guid: 17fa069a-480b-11df-badc-005056a7121f
    read_only:
    set_data:
      :notes: This policy profile analyzes a vm's configuration data when it's reconfigured
        an sends an email if the cpu reservation is set to a value greater than 500.
    mode: control
    owner_type:
    owner_id:
    MiqPolicy:
  - name: 2f2a1alc-4806-11df-badc-005056a7121f
    description: ! 'Analysis: VM Reconfiguration'
    expression:
    towhat: Vm
    guid: 2f2a1alc-4806-11df-badc-005056a7121f
    created_by: admin
    updated_by: admin
    notes: Performs an analysis on any vm that has been reconfigured
    active: true
    mode: control
    MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_reconfigure
      description: VM Settings Change

```

```

    guid: 07367e62-449a-11de-bd4f-005056a83e5d
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: vm_analyze
    description: Initiate SmartState Analysis for VM
    guid: 5cbe1082-ce35-11de-a117-005056b0503e
    action_type: default
    options: {}
  Condition: []
- name: 8a8f247a-480a-11df-badc-005056a7121f
  description: ! 'Configuration: VM - CPU Reservation > 500Mhz'
  expression:
  towhat: Vm
  guid: 8a8f247a-480a-11df-badc-005056a7121f
  created_by: admin
  updated_by: admin
  notes: Sends an email if CPU reservation is set to a value greater than 500Mhz
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
  MiqEvent:
    name: vm_scan_complete
    description: VM Analysis Complete
    guid: f7b8361e-1139-11e1-9333-005056af009e
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: 5189755e-480a-11df-badc-005056a7121f
    description: Alert - CPU Reservation > 500Mhz
    guid: 5189755e-480a-11df-badc-005056a7121f
    action_type: evaluate_alerts
    options:
      :alert_guids:
      - ca26a9c6-4802-11df-badc-005056a7121f
  Condition: []
- name: 467f80ce-4808-11df-badc-005056a7121f
  description: ! 'Analysis: VM Configuration Only Profile'
  expression:
  towhat: Vm
  guid: 467f80ce-4808-11df-badc-005056a7121f
  created_by: admin
  updated_by: admin
  notes: ! 'This policy assigns an analysis profile that only gathers vm configuration
    data. Note: the specified action requires that you create an analysis profile
    that only scans vm configuration data. Once it has been created, associate
    it with the specified action'
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
  MiqEvent:

```

```

    name: vm_scan_start
    description: VM Analysis Start
    guid: 057b9baa-519c-11e0-8d82-005056af0000
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: b52a86f0-4807-11df-badc-005056a7121f
    description: ! 'Profile: VM configuration only'
    guid: b52a86f0-4807-11df-badc-005056a7121f
    action_type: assign_scan_profile
    options:
      :scan_item_set_name: vm configuration only
  Condition: []
- MiqPolicySet:
  name: 6fb380a4-3b86-11e0-9dc0-005056910001
  description: ! 'Demo: Prevent Cloning of Database VMs '
  set_type: MiqPolicySet
  guid: 6fb380a4-3b86-11e0-9dc0-005056910001
  read_only:
  set_data:
    :notes: This policy prevents any vm with a workload tag of database from being
      cloned
  mode: control
  owner_type:
  owner_id:
  MiqPolicy:
  - name: Configuration Policy Restrict Cloning SQL Server
    description: ! 'Operational: Prevent Cloning of Database VMs'
    expression:
    towhat: Vm
    guid: 39fdeba0-2866-11de-af2a-0050568026c2
    created_by:
    updated_by: admin
    notes: prevents cloning of vms with a workload tag value of database
    active: true
    mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
  MiqEvent:
    name: vm_clone_start
    description: VM Clone Start
    guid: e30f6720-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: cancel_task
    description: Cancel vCenter Task
    guid: e49bfee6-1e1e-11de-8918-0050568005db
    action_type: default
    options: {}
  - qualifier: success
    success_sequence: 2
  MiqEvent:
    name: vm_clone_start

```



[illegible]

```

action_type: set_custom_attribute
options:
  :variables:
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: Clone Prevented for SQL Server VM
      :attribute: EVM Policy
Condition:
- name: VMs running SQL Server
  description: VMs with Workload - Database
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      CONTAINS:
        tag: Vm.managed-function
        value: database
      context_type:
        towhat: Vm
        file_mtime:
          guid: 121ecf62-01c6-11de-a701-005056903dbc
          filename:
            applies_to_exp:
              miq_policy_id: 100000000000064
            notes:
- MiqPolicySet:
  name: 3b818590-2866-11de-af2a-0050568026c2
  description: ! 'Demo: Service Level Resource Allocation'
  set_type: MiqPolicySet
  guid: 3b818590-2866-11de-af2a-0050568026c2
  read_only:
  set_data:
```

```

:notes: This policy demonstrates EVM's ability to check and , if necessary,
reconfigure a VM's vCPU and Memory configuration based on designated service
level
mode: control
owner_type:
owner_id:
MiqPolicy:
- name: d16643b6-3905-11de-b6d5-005056a11a54
description: Service Level Silver - RAM must be 512MB and 1 vCPU - on
expression: !ruby/object:MiqExpression
exp:
and:
- CONTAINS:
tag: Vm.managed-service_level
value: silver
- =:
value: 'on'
field: Vm-power_state
context_type:
towhat: Vm
guid: d16643b6-3905-11de-b6d5-005056a11a54
created_by:
updated_by: admin
notes: This policy verifies that a vm that has a service level tag of silver
has 1 vCPU and 512MB of memory. If not it changes the vm to these values.
This policy is used on a powered on vm.
active: true
mode: control
MiqPolicyContent:
- qualifier: success
success_sequence: 1
MiqEvent:
name: assigned_company_tag
description: Tag Complete
guid: e384ecb6-1e1e-11de-8918-0050568005db
event_type: Default
definition:
default:
enabled:
MiqAction:
name: vm_stop
description: Stop Virtual Machine
guid: 37f2da3e-21a8-11e2-b47a-0050568b19a3
action_type: default
options: {}
- qualifier: success
success_sequence: 2
MiqEvent:
name: assigned_company_tag
description: Tag Complete
guid: e384ecb6-1e1e-11de-8918-0050568005db
event_type: Default
definition:
default:
enabled:
MiqAction:
name: VM_RAM_512MB
description: Set VM RAM to 512MB
guid: bab04cb4-9af1-11dd-8e55-005056ac7d2c

```

```

    action_type: reconfigure_memory
    options:
      :value: 512
- qualifier: success
  success_sequence: 3
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1ele-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: VM_CPU_1
    description: Set VM CPU to 1
    guid: d97dafba-9af1-11dd-8e55-005056ac7d2c
    action_type: reconfigure_cpus
    options:
      :value: '1'
- qualifier: success
  success_sequence: 4
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1ele-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: vm_start
    description: Start Virtual Machine
    guid: 55b5a422-3348-11de-bde2-005056a170fa
    action_type: default
    options: {}
  Condition:
- name: Service Level Validation Silver - Powered Off
  description: Service Level Silver - VM RAM and CPU check
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      or:
      - ! '!=':
          value: 512
          field: Vm.hardware-memory_cpu
      - ! '!=':
          value: 1
          field: Vm.hardware-numvcpus
  towhat: Vm
  file_mtime:
  guid: 531575ae-9b1c-11dd-bbd7-005056ac7d2c
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000068
  notes:
- name: 4cb4d05c-3909-11de-b6d5-005056a11a54
  description: Service Level Platinum - RAM must be 2GB and 2 vCPUs - on
  expression: !ruby/object:MiqExpression

```

```

exp:
  and:
    - CONTAINS:
      tag: Vm.managed-service_level
      value: platinum
    - =:
      value: 'on'
      field: Vm-power_state
  context_type:
towhat: Vm
guid: 4cb4d05c-3909-11de-b6d5-005056a11a54
created_by:
updated_by: admin
notes: This policy verifies that a vm that has a service level tag of platinum
      has 2 vCPUs and 2GB of memory. If not it changes the vm to these values. This
      policy is used on a powered on vm.
active: true
mode: control
MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: vm_stop
    description: Stop Virtual Machine
    guid: 37f2da3e-21a8-11e2-b47a-0050568b19a3
    action_type: default
    options: {}
- qualifier: success
  success_sequence: 2
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: VM_RAM_2GB
    description: Set VM RAM to 2GB
    guid: cf1570b2-9af1-11dd-8e55-005056ac7d2c
    action_type: reconfigure_memory
    options:
      :value: 2048
- qualifier: success
  success_sequence: 3
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default

```

```

    definition:
    default:
    enabled:
  MiqAction:
    name: VM_CPU_2
    description: Set VM CPU to 2
    guid: e2c3d64e-9af1-11dd-8e55-005056ac7d2c
    action_type: reconfigure_cpus
    options:
      :value: '2'
- qualifier: success
  success_sequence: 4
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: vm_start
    description: Start Virtual Machine
    guid: 55b5a422-3348-11de-bde2-005056a170fa
    action_type: default
    options: {}
  Condition:
- name: 34218558-3909-11de-b6d5-005056a11a54
  description: Service Level Platinum - VM RAM and CPU check
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      or:
        - ! '!=':
            value: 2048
            field: Vm.hardware-memory_cpu
        - ! '!=':
            value: 2
            field: Vm.hardware-numvcpus
  towhat: Vm
  file_mtime:
  guid: 34218558-3909-11de-b6d5-005056a11a54
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000070
  notes:
- name: 7a91f3ac-3908-11de-b6d5-005056a11a54
  description: Service Level Gold - RAM must be 1GB and 1 vCPU - on
  expression: !ruby/object:MiqExpression
    exp:
      and:
        - CONTAINS:
            tag: Vm.managed-service_level
            value: gold
        - =:
            value: 'on'
            field: Vm-power_state
  context_type:
  towhat: Vm

```

```
guid: 7a91f3ac-3908-11de-b6d5-005056a11a54
created_by:
updated_by: admin
notes: This policy verifies that a vm that has a service level tag of gold has
      1vCPU and 1GB of memory. If not it changes the vm to these values. This policy
      is used on a powered on vm.
active: true
mode: control
MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: vm_stop
    description: Stop Virtual Machine
    guid: 37f2da3e-21a8-11e2-b47a-0050568b19a3
    action_type: default
    options: {}
- qualifier: success
  success_sequence: 2
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: VM_RAM_1GB
    description: Set VM RAM to 1GB
    guid: 2d8445f2-9aec-11dd-8e55-005056ac7d2c
    action_type: reconfigure_memory
    options:
      :value: 1024
- qualifier: success
  success_sequence: 3
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: VM_CPU_1
    description: Set VM CPU to 1
    guid: d97dafba-9afl-11dd-8e55-005056ac7d2c
    action_type: reconfigure_cpus
    options:
      :value: '1'
```

```

- qualifier: success
  success_sequence: 4
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
        enabled:
  MiqAction:
    name: vm_start
    description: Start Virtual Machine
    guid: 55b5a422-3348-11de-bde2-005056a170fa
    action_type: default
    options: {}
  Condition:
- name: 1c6ec35e-3908-11de-b6d5-005056a11a54
  description: Service Level Gold - VM RAM and CPU check
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      or:
        - ! '!=':
            value: 1024
            field: Vm.hardware-memory_cpu
        - ! '!=':
            value: 1
            field: Vm.hardware-numvcpus
  towhat: Vm
  file_mtime:
  guid: 1c6ec35e-3908-11de-b6d5-005056a11a54
  filename:
  applies_to_exp:
  miq_policy_id: 100000000000069
  notes:
- name: Service Level Policy Verify Virtual Hardware - Silver Level
  description: Service Level Silver - RAM must be 512MB and 1 vCPU - off
  expression: !ruby/object:MiqExpression
    exp:
      and:
        - CONTAINS:
            tag: Vm.managed-service_level
            value: silver
        - =:
            value: 'off'
            field: Vm-power_state
      context_type:
  towhat: Vm
  guid: 3659b8bc-2866-11de-af2a-0050568026c2
  created_by:
  updated_by: admin
  notes: This policy verifies that a vm that has a service level tag of silver
    has 1 vCPU and 512MB of memory. If not it changes the vm to these values.
    This policy is used on a powered off vm.
  active: true
  mode: control
  MiqPolicyContent:
- qualifier: success

```



```

    success_sequence: 1
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: VM_CPU_1
    description: Set VM CPU to 1
    guid: d97dafba-9af1-11dd-8e55-005056ac7d2c
    action_type: reconfigure_cpus
    options:
      :value: '1'
- qualifier: success
  success_sequence: 2
  MiqEvent:
    name: assigned_company_tag
    description: Tag Complete
    guid: e384ecb6-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: VM_RAM_512MB
    description: Set VM RAM to 512MB
    guid: bab04cb4-9af1-11dd-8e55-005056ac7d2c
    action_type: reconfigure_memory
    options:
      :value: 512
  Condition:
- name: Service Level Validation Silver - Powered Off
  description: Service Level Silver - VM RAM and CPU check
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      or:
      - ! '!=':
          value: 512
          field: Vm.hardware-memory_cpu
      - ! '!=':
          value: 1
          field: Vm.hardware-numvcpus
  towhat: Vm
  file_mtime:
  guid: 531575ae-9b1c-11dd-bbd7-005056ac7d2c
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000068
  notes:
- name: 24b92088-399c-11de-ae27-005056a11a54
  description: Service Level Gold - RAM must be 1GB and 1 vCPU - off
  expression: !ruby/object:MiqExpression
    exp:
      and:
      - CONTAINS:

```

```

      tag: Vm.managed-service_level
      value: gold
    - =:
      value: 'off'
      field: Vm-power_state
    context_type:
  towhat: Vm
  guid: 24b92088-399c-11de-ae27-005056a11a54
  created_by:
  updated_by: admin
  notes: This policy verifies that a vm that has a service level tag of gold has
    1vCPU and 1GB of memory. If not it changes the vm to these values. This policy
    is used on a powered off vm.
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: assigned_company_tag
      description: Tag Complete
      guid: e384ecb6-1e1e-11de-8918-0050568005db
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: VM_RAM_1GB
      description: Set VM RAM to 1GB
      guid: 2d8445f2-9aec-11dd-8e55-005056ac7d2c
      action_type: reconfigure_memory
      options:
        :value: 1024
  - qualifier: success
    success_sequence: 2
    MiqEvent:
      name: assigned_company_tag
      description: Tag Complete
      guid: e384ecb6-1e1e-11de-8918-0050568005db
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: VM_CPU_1
      description: Set VM CPU to 1
      guid: d97dafba-9af1-11dd-8e55-005056ac7d2c
      action_type: reconfigure_cpus
      options:
        :value: '1'
  Condition:
  - name: 1c6ec35e-3908-11de-b6d5-005056a11a54
    description: Service Level Gold - VM RAM and CPU check
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        or:
          - ! '!=':
            value: 1024

```

```

      field: Vm.hardware-memory_cpu
    - ! '!=':
      value: 1
      field: Vm.hardware-numvcpus
  towhat: Vm
  file_mtime:
  guid: 1c6ec35e-3908-11de-b6d5-005056a11a54
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000069
  notes:
- name: b265c970-3908-11de-b6d5-005056a11a54
  description: Service Level Platinum - RAM must be 2GB and 2 vCPUs - off
  expression: !ruby/object:MiqExpression
    exp:
      and:
      - CONTAINS:
        tag: Vm.managed-service_level
        value: platinum
      - =:
        value: 'off'
        field: Vm-power_state
    context_type:
  towhat: Vm
  guid: b265c970-3908-11de-b6d5-005056a11a54
  created_by:
  updated_by: admin
  notes: This policy verifies that a vm that has a service level tag of platinum
    has 2 vCPUs and 2GB of memory. If not it changes the vm to these values. This
    policy is used on a powered off vm.
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: assigned_company_tag
      description: Tag Complete
      guid: e384ecb6-1e1e-11de-8918-0050568005db
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: VM_RAM_2GB
      description: Set VM RAM to 2GB
      guid: cf1570b2-9af1-11dd-8e55-005056ac7d2c
      action_type: reconfigure_memory
      options:
        :value: 2048
  - qualifier: success
    success_sequence: 2
    MiqEvent:
      name: assigned_company_tag
      description: Tag Complete
      guid: e384ecb6-1e1e-11de-8918-0050568005db
      event_type: Default
      definition:
        default:

```

```

    enabled:
  MiqAction:
    name: VM_CPU_2
    description: Set VM CPU to 2
    guid: e2c3d64e-9af1-11dd-8e55-005056ac7d2c
    action_type: reconfigure_cpus
    options:
      :value: '2'
  Condition:
  - name: 34218558-3909-11de-b6d5-005056a11a54
    description: Service Level Platinum - VM RAM and CPU check
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        or:
        - ! '!=':
            value: 2048
            field: Vm.hardware-memory_cpu
        - ! '!=':
            value: 2
            field: Vm.hardware-numvcpus
    towhat: Vm
    file_mtime:
    guid: 34218558-3909-11de-b6d5-005056a11a54
    filename:
    applies_to_exp:
    miq_policy_id: 10000000000070
    notes:
- MiqPolicySet:
  name: fc164798-3b81-11e0-9dc0-005056910001
  description: ! 'Demo: Windows Mandatory Patch'
  set_type: MiqPolicySet
  guid: fc164798-3b81-11e0-9dc0-005056910001
  read_only:
  set_data:
  mode: control
  owner_type:
  owner_id:
  MiqPolicy:
  - name: c5d44cb2-4734-11df-b577-005056a7121f
    description: ! 'Patch: MS10-008 Required'
    expression: !ruby/object:MiqExpression
      exp:
        CONTAINS:
          tag: Vm.managed-environment
          value: prod
        context_type:
    towhat: Vm
    guid: c5d44cb2-4734-11df-b577-005056a7121f
    created_by: admin
    updated_by: admin
    notes: Prevents a VM that does not have MS10-008 installed from running in the
      virtual environment. It's scope limits it to vms tagged as production
    active: true
    mode: control
    MiqPolicyContent:
      - qualifier: failure
        failure_sequence: 1
    MiqEvent:

```

[illegible]

```

      :var_type: <None>
      :from: evmadmin@manageiq.com
      :to: evm_demo@manageiq.com
- qualifier: failure
  failure_sequence: 3
  MiqEvent:
    name: vm_start
    description: VM Power On
    guid: 404b4630-21a8-11e2-b47a-0050568b19a3
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: 722d25cc-56dc-11df-bb16-005056a7121f
    description: VM Attribute - Fails patch policy
    guid: 722d25cc-56dc-11df-bb16-005056a7121f
    action_type: set_custom_attribute
    options:
      :variables:
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      :value: Failed Windows Required Patch Policy
      :attribute: EVM Policy
  Condition:
  - name: a3089008-4734-11df-b577-005056a7121f
    description: Verify KB978262 is installed
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        CONTAINS:

```

```

        value: KB978262
        field: Vm.patches-name
        context_type:
        towhat: Vm
        file_mtime:
        guid: a3089008-4734-11df-b577-005056a7121f
        filename:
        applies_to_exp:
        miq_policy_id: 100000000000071
        notes:
- MiqPolicySet:
  name: 3be240d8-2866-11de-af2a-0050568026c2
  description: ! 'Mandatory: Provisioning and Retirement'
  set_type: MiqPolicySet
  guid: 3be240d8-2866-11de-af2a-0050568026c2
  read_only:
  set_data:
    :notes: ! 'This policy profile is REQUIRED if EVM is being used to Provision
      or Retire vms. It must be entitled to the desired management systems. Note:
      this policy profile will potentially result in the removal of a vm from the
      management system upon retirement if the associated VM Retirement statemachine
      [/Factory/StateMachine/VMRetirement] in the the Automate model is configured
      to delete vms. It is not configured for vm deletion out-of-the-box.'
  mode: control
  owner_type:
  owner_id:
  MiqPolicy:
- name: Automation Policy - Scope VM Retired Response Execute Automation Model
  description: ! 'Operational: Vm Retired'
  expression:
  towhat: Vm
  guid: 397700ae-2866-11de-af2a-0050568026c2
  created_by:
  updated_by: admin
  notes: This policy raises an automation event when a vm retirement event is
    raised
  active: true
  mode: control
  MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  failure_synchronous: true
  MiqEvent:
    name: vm_retired
    description: VM Retired
    guid: e363d8aa-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: raise_automation_event
    description: Raise Automation Event
    guid: e7da3b7a-1139-11e1-9333-005056af009e
    action_type: default
    options: {}
  Condition: []
- name: Automation Policy - Scope VM Retirement Warning, ResponseExecute Automation
  Model

```

```

description: ! 'Operational: Retirement Warning'
expression:
towhat: Vm
guid: 39621392-2866-11de-af2a-0050568026c2
created_by:
updated_by: admin
notes: This policy raises an automation event when a retirement warning event
      is raised
active: true
mode: control
MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  failure_synchronous: true
  MiqEvent:
    name: vm_retire_warn
    description: VM Retirement Warning
    guid: 97c85330-fe93-11dd-b5e1-005056903dbc
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: raise_automation_event
    description: Raise Automation Event
    guid: e7da3b7a-1139-11e1-9333-005056af009e
    action_type: default
    options: {}
  Condition: []
- name: 427a4378-6519-11df-b637-005056a435be
  description: ! 'Analysis: Post Provisioning'
  expression:
towhat: Vm
guid: 427a4378-6519-11df-b637-005056a435be
created_by: admin
updated_by: admin
notes: This policy triggers a vm analysis of any newly provisioned VM
active: true
mode: control
MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_provisioned
    description: VM Provision Complete
    guid: 2a17a20a-3e8e-11df-9fe2-005056a435be
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: vm_analyze
    description: Initiate SmartState Analysis for VM
    guid: 5cbe1082-ce35-11de-a117-005056b0503e
    action_type: default
    options: {}
  Condition: []
- MiqPolicySet:
  name: 63aaa3aa-53fa-11e0-babf-00505688000a

```



```

description: ! 'Operational: Prevent Cloning of Database VMs'
set_type: MiqPolicySet
guid: 63aaa3aa-53fa-11e0-babf-00505688000a
read_only:
set_data:
  :notes: This policy profile prevents database vms from being cloned. Database
    vms are defined as those that have a workload tag value of database
mode: control
owner_type:
owner_id:
MiqPolicy:
- name: Configuration Policy Restrict Cloning SQL Server
  description: ! 'Operational: Prevent Cloning of Database VMs'
  expression:
  towhat: Vm
  guid: 39fdeba0-2866-11de-af2a-0050568026c2
  created_by:
  updated_by: admin
  notes: prevents cloning of vms with a workload tag value of database
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_clone_start
      description: VM Clone Start
      guid: e30f6720-1e1e-11de-8918-0050568005db
      event_type: Default
      definition:
      default:
      enabled:
    MiqAction:
      name: cancel_task
      description: Cancel vCenter Task
      guid: e49bfee6-1e1e-11de-8918-0050568005db
      action_type: default
      options: {}
  - qualifier: success
    success_sequence: 2
    MiqEvent:
      name: vm_clone_start
      description: VM Clone Start
      guid: e30f6720-1e1e-11de-8918-0050568005db
      event_type: Default
      definition:
      default:
      enabled:
    MiqAction:
      name: SendEmail
      description: SendEmail
      guid: abcf406c-02cd-11de-86d4-005056903dbc
      action_type: email
      options:
        :variables:
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''

```

```

      :oid: ''
      :var_type: <None>
-   :value: ''
      :oid: ''
      :var_type: <None>
-   :value: ''
      :oid: ''
      :var_type: <None>
-   :value: ''
      :oid: ''
      :var_type: <None>
-   :value: ''
      :oid: ''
      :var_type: <None>
-   :value: ''
      :oid: ''
      :var_type: <None>
-   :value: ''
      :oid: ''
      :var_type: <None>
-   :value: ''
      :oid: ''
      :var_type: <None>
      :from: evmadmin@manageiq.com
      :to: evm_demo@manageiq.com
-   qualifier: success
      success_sequence: 3
MiqEvent:
  name: vm_clone_start
  description: VM Clone Start
  guid: e30f6720-1e1e-11de-8918-0050568005db
  event_type: Default
  definition:
    default:
    enabled:
MiqAction:
  name: 4468f036-0b6d-11df-bd07-005056a7121f
  description: VM Attribute - Prevent Clone of SQL Server
  guid: 4468f036-0b6d-11df-bd07-005056a7121f
  action_type: set_custom_attribute
  options:
    :variables:
-   :value: ''
      :oid: ''
      :var_type: <None>
-   :value: ''
      :oid: ''
      :var_type: <None>
-   :value: ''
      :oid: ''
      :var_type: <None>
-   :value: ''
      :oid: ''
      :var_type: <None>
-   :value: ''
      :oid: ''
      :var_type: <None>
-   :value: ''
      :oid: ''

```

```

      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    :value: Clone Prevented for SQL Server VM
    :attribute: EVM Policy
Condition:
- name: VMs running SQL Server
  description: VMs with Workload - Database
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      CONTAINS:
        tag: Vm.managed-function
        value: database
      context_type:
        towhat: Vm
        file_mtime:
        guid: 121ecf62-01c6-11de-a701-005056903dbc
        filename:
        applies_to_exp:
        miq_policy_id: 100000000000064
        notes:
- MiqPolicySet:
  name: 97fe0866-b8e5-11e2-87c6-001a4a034c7a
  description: RHEL + KVM
  set_type: MiqPolicySet
  guid: 97fe0866-b8e5-11e2-87c6-001a4a034c7a
  read_only:
  set_data:
  mode: control
  owner_type:
  owner_id:
  MiqPolicy:
- name: c63b0560-fa45-11de-83ca-005056ba0614
  description: Root Login via SSH should be Disabled
  expression:
  towhat: Host
  guid: c63b0560-fa45-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that the root account cannot login to the host via
    SSH.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure

```

```

failure_sequence: 1
MiqEvent:
  name: host_compliance_check
  description: Host Compliance Check
  guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
  event_type: Default
  definition:
    default:
    enabled:
MiqAction:
  name: compliance_failed
  description: Mark as Non-Compliant
  guid: ba452d94-f586-11de-8ebc-0050568a07c7
  action_type: default
  options: {}
Condition:
- name: 4435b6d6-fa46-11de-83ca-005056ba0614
  description: PermitRootLogin = no in sshd_config file
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^\s*PermitRootLogin\s+no
            field: Host.filesystems-contents
        search:
          =:
            value: /etc/ssh/sshd_config
            field: Host.filesystems-name
        towhat: Host
        file_mtime:
        guid: 4435b6d6-fa46-11de-83ca-005056ba0614
        filename:
        applies_to_exp:
        miq_policy_id: 10000000000042
        notes: This condition checks the file /etc/ssh/sshd_config and verifies that
              the PermitRootLogin parameter's value is set to no.
- name: af2d74ea-fa39-11de-83ca-005056ba0614
  description: Firewall - Incoming Security Level
  expression:
  towhat: Host
  guid: af2d74ea-fa39-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that only a defined set of incoming TCP and UDP
        Ports are open.
  active: true
  mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
    MiqEvent:
      name: host_compliance_check
      description: Host Compliance Check
      guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
      event_type: Default
      definition:
        default:

```

```

    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: b4a0843a-fa43-11de-83ca-005056ba0614
    description: Valid Incoming UDP Ports
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        LIMITED TO:
          value: '427'
          field: Host-enabled_udp_inbound_ports
    towhat: Host
    file_mtime:
    guid: b4a0843a-fa43-11de-83ca-005056ba0614
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000021
    notes: This condition verifies that the only open incoming UDP port is 427.
  - name: 03529e9e-f961-11de-9e9d-0050568a07c7
    description: Valid Incoming TCP Ports
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        LIMITED TO:
          value: '902,80,443,427,5989,22,5988'
          field: Host-enabled_tcp_inbound_ports
    towhat: Host
    file_mtime:
    guid: 03529e9e-f961-11de-9e9d-0050568a07c7
    filename:
    applies_to_exp:
    miq_policy_id: 100000000000021
    notes: This condition verifies that the only open incoming TCP ports are ↔
      22,80,427,443,902,5988,and
      5989.
  - name: 04db603c-fa3a-11de-83ca-005056ba0614
    description: Firewall - Outgoing Security Level
    expression:
    towhat: Host
    guid: 04db603c-fa3a-11de-83ca-005056ba0614
    created_by: admin
    updated_by: admin
    notes: This policy verifies that only a defined set of outgoing TCP and UDP
      Ports are open.
    active: true
    mode: compliance
  MiqPolicyContent:
  - qualifier: failure
    failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default

```

```

    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
- name: f0afd7d6-fa3a-11de-83ca-005056ba0614
  description: Valid Outgoing TCP Ports
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      LIMITED TO:
        value: '902,427,443,27000,27010'
        field: Host-enabled_tcp_outbound_ports
  towhat: Host
  file_mtime:
  guid: f0afd7d6-fa3a-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000020
  notes: This condition verifies that the only open outgoing TCP ports are ↵
    427,443,902,27000,
    and 27010.
- name: 1778fb28-fa44-11de-83ca-005056ba0614
  description: Valid Outgoing UDP Ports
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      LIMITED TO:
        value: '427,123,902'
        field: Host-enabled_udp_outbound_ports
  towhat: Host
  file_mtime:
  guid: 1778fb28-fa44-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 10000000000020
  notes: This condition verifies that the only open outgoing UDP ports are 123,427,
    and 902.
- name: 8cecc84c-fa46-11de-83ca-005056ba0614
  description: Limit su Access to root Account
  expression:
  towhat: Host
  guid: 8cecc84c-fa46-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy validates that only members of the group wheel can access
    the su command.
  active: true
  mode: compliance
  MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: host_compliance_check

```

```

    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed
    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
- name: 63b243fc-fa47-11de-83ca-005056ba0614
  description: Only members of wheel group can execute su command
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      FIND:
        checkany:
          REGULAR EXPRESSION MATCHES:
            value: ^\s*auth\s+required\s+.*pam_wheel\.so\s+use_uid
            field: Host.filesystems-contents
        search:
          =:
            value: /etc/pam.d/su
            field: Host.filesystems-name
  towhat: Host
  file_mtime:
  guid: 63b243fc-fa47-11de-83ca-005056ba0614
  filename:
  applies_to_exp:
  miq_policy_id: 100000000000050
  notes: This condition validates that the file /etc/pam.d/su contains a variation
    of the string "auth required pam_wheel.so use_uid".
- name: 4ed279b2-fa55-11de-83ca-005056ba0614
  description: Timekeeping - NTP Service Running
  expression:
  towhat: Host
  guid: 4ed279b2-fa55-11de-83ca-005056ba0614
  created_by: admin
  updated_by: admin
  notes: This policy verifies that the NTP servers is configured to automatically
    start.
  active: true
  mode: compliance
  MiqPolicyContent:
- qualifier: failure
  failure_sequence: 1
  MiqEvent:
    name: host_compliance_check
    description: Host Compliance Check
    guid: b9abe0a8-f586-11de-8ebc-0050568a07c7
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: compliance_failed

```

```

    description: Mark as Non-Compliant
    guid: ba452d94-f586-11de-8ebc-0050568a07c7
    action_type: default
    options: {}
  Condition:
  - name: 9a08d21e-fa55-11de-83ca-005056ba0614
    description: Verify NTP is Running
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          checkany:
            INCLUDES:
              value: '3'
              field: Host.host_services-enable_run_levels
          search:
            =:
              value: ntpd
              field: Host.host_services-name
          towhat: Host
          file_mtime:
            guid: 9a08d21e-fa55-11de-83ca-005056ba0614
            filename:
              applies_to_exp:
                miq_policy_id: 10000000000031
            notes: This condition verifies that the run level of the service ntpd is set
                  to three.
  - MiqPolicySet:
    name: 51149d78-cb15-11e3-b1c5-001a4a0f459e
    description: Resolv.conf
    set_type: MiqPolicySet
    guid: 51149d78-cb15-11e3-b1c5-001a4a0f459e
    read_only:
    set_data:
    mode: control
    owner_type:
    owner_id:
    MiqPolicy:
  - name: e3f6428c-a85a-11e3-9c44-001a4a0f459e
    description: Settings - /etc/resolv.conf
    expression: !ruby/object:MiqExpression
      exp:
        FIND:
          search:
            =:
              field: Vm.filesystems-name
              value: resolv.conf
          checkall:
            =:
              field: Vm.filesystems-contents_available
              value: 'true'
        context_type:
      towhat: Vm
    guid: e3f6428c-a85a-11e3-9c44-001a4a0f459e
    created_by: admin
    updated_by: admin
    notes:
    active: true
    mode: compliance

```



```
MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  success_synchronous: true
  MiqEvent:
    name: vm_compliance_check
    description: VM Compliance Check
    guid: 816a598a-f57d-11de-a41a-005056ba0614
    event_type: Default
    definition:
      default:
        enabled:
  MiqAction:
    name: log
    description: Generate log message
    guid: 04771f80-431c-11e3-91d5-001a4a0f459e
    action_type: default
    options: {}
- qualifier: success
  success_sequence: 2
  success_synchronous: true
  MiqEvent:
    name: vm_compliance_check
    description: VM Compliance Check
    guid: 816a598a-f57d-11de-a41a-005056ba0614
    event_type: Default
    definition:
      default:
        enabled:
  MiqAction:
    name: c26b7988-a860-11e3-9c44-001a4a0f459e
    description: resolv.conf
    guid: c26b7988-a860-11e3-9c44-001a4a0f459e
    action_type: custom_automation
    options:
      :ae_request: resolvsend
      :ae_message: create
- qualifier: failure
  failure_sequence: 1
  failure_synchronous: true
  MiqEvent:
    name: vm_compliance_check
    description: VM Compliance Check
    guid: 816a598a-f57d-11de-a41a-005056ba0614
    event_type: Default
    definition:
      default:
        enabled:
  MiqAction:
    name: log
    description: Generate log message
    guid: 04771f80-431c-11e3-91d5-001a4a0f459e
    action_type: default
    options: {}
  Condition: []
- MiqPolicySet:
  name: 5a7d53b4-53f9-11e0-babf-00505688000a
  description: ! 'Snapshot Management: Delete Based On Count'
  set_type: MiqPolicySet
```

```

guid: 5a7d53b4-53f9-11e0-babf-00505688000a
read_only:
set_data:
  :notes: This policy profile deletes the most recent snapshot when more that
    2 snapshots exists
mode: control
owner_type:
owner_id:
MiqPolicy:
- name: 994efe7e-18e6-11e0-88b4-005056a7184a
  description: ! 'Snapshots: Delete based on Count'
  expression:
  towhat: Vm
  guid: 994efe7e-18e6-11e0-88b4-005056a7184a
  created_by: admin
  updated_by: admin
  notes: This policy deletes the most recent snapshot when more that 2 snapshots
    exists
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_snapshot_complete
      description: VM Snapshot Create Complete
      guid: 7eb82802-135e-11e0-8706-005056a7184a
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: delete_most_recent_snapshot
      description: Delete Most Recent Snapshot
      guid: 7f6e2f8a-135e-11e0-8706-005056a7184a
      action_type: default
      options: {}
  Condition:
  - name: 992035fc-18e7-11e0-88b4-005056a7184a
    description: Check for more than 2 snapshots
    modifier: allow
    expression: !ruby/object:MiqExpression
      exp:
        ! '>':
          value: '2'
          field: Vm-v_total_snapshots
        context_type:
        towhat: Vm
        file_mtime:
        guid: 992035fc-18e7-11e0-88b4-005056a7184a
        filename:
        applies_to_exp:
        miq_policy_id: 100000000000075
        notes: Checks to see if more than 2 snapshots exist
- MiqPolicySet:
  name: 05b51354-53fd-11e0-babf-00505688000a
  description: Standards
  set_type: MiqPolicySet
  guid: 05b51354-53fd-11e0-babf-00505688000a

```

```

read_only:
set_data:
  :notes: This policy profile is an example of creation of a single profile that
    contains all policies that should be enforced on all objects in the environment.
mode: control
owner_type:
owner_id:
MiqPolicy:
- name: Configuration Policy Restrict Cloning SQL Server
  description: ! 'Operational: Prevent Cloning of Database VMs'
  expression:
  towhat: Vm
  guid: 39fdeba0-2866-11de-af2a-0050568026c2
  created_by:
  updated_by: admin
  notes: prevents cloning of vms with a workload tag value of database
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_clone_start
      description: VM Clone Start
      guid: e30f6720-1e1e-11de-8918-0050568005db
      event_type: Default
      definition:
      default:
      enabled:
    MiqAction:
      name: cancel_task
      description: Cancel vCenter Task
      guid: e49bfee6-1e1e-11de-8918-0050568005db
      action_type: default
      options: {}
  - qualifier: success
    success_sequence: 2
    MiqEvent:
      name: vm_clone_start
      description: VM Clone Start
      guid: e30f6720-1e1e-11de-8918-0050568005db
      event_type: Default
      definition:
      default:
      enabled:
    MiqAction:
      name: SendEmail
      description: SendEmail
      guid: abcf406c-02cd-11de-86d4-005056903dbc
      action_type: email
      options:
        :variables:
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''
          :oid: ''
          :var_type: <None>
        - :value: ''

```

```

      :oid: ''
      :var_type: <None>
- :value: ''
      :oid: ''
      :var_type: <None>
- :value: ''
      :oid: ''
      :var_type: <None>
- :value: ''
      :oid: ''
      :var_type: <None>
- :value: ''
      :oid: ''
      :var_type: <None>
- :value: ''
      :oid: ''
      :var_type: <None>
- :value: ''
      :oid: ''
      :var_type: <None>
      :from: evmadmin@manageiq.com
      :to: evm_demo@manageiq.com
- qualifier: success
  success_sequence: 3
  MiqEvent:
    name: vm_clone_start
    description: VM Clone Start
    guid: e30f6720-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: 4468f036-0b6d-11df-bd07-005056a7121f
    description: VM Attribute - Prevent Clone of SQL Server
    guid: 4468f036-0b6d-11df-bd07-005056a7121f
    action_type: set_custom_attribute
    options:
      :variables:
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''
        :var_type: <None>
      - :value: ''
        :oid: ''

```

```

      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    - :value: ''
      :oid: ''
      :var_type: <None>
    :value: Clone Prevented for SQL Server VM
    :attribute: EVM Policy
Condition:
- name: VMs running SQL Server
  description: VMs with Workload - Database
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      CONTAINS:
        tag: Vm.managed-function
        value: database
      context_type:
        towhat: Vm
        file_mtime:
        guid: 121ecf62-01c6-11de-a701-005056903dbc
        filename:
        applies_to_exp:
        miq_policy_id: 100000000000064
        notes:
- name: 994efe7e-18e6-11e0-88b4-005056a7184a
  description: ! 'Snapshots: Delete based on Count'
  expression:
  towhat: Vm
  guid: 994efe7e-18e6-11e0-88b4-005056a7184a
  created_by: admin
  updated_by: admin
  notes: This policy deletes the most recent snapshot when more that 2 snapshots
    exists
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_snapshot_complete
      description: VM Snapshot Create Complete
      guid: 7eb82802-135e-11e0-8706-005056a7184a
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: delete_most_recent_snapshot
      description: Delete Most Recent Snapshot
      guid: 7f6e2f8a-135e-11e0-8706-005056a7184a
      action_type: default

```

```

      options: {}
    Condition:
    - name: 992035fc-18e7-11e0-88b4-005056a7184a
      description: Check for more than 2 snapshots
      modifier: allow
      expression: !ruby/object:MiqExpression
        exp:
          ! '>':
            value: '2'
            field: Vm-v_total_snapshots
          context_type:
            towhat: Vm
            file_mtime:
            guid: 992035fc-18e7-11e0-88b4-005056a7184a
            filename:
            applies_to_exp:
            miq_policy_id: 100000000000075
            notes: Checks to see if more than 2 snapshots exist
    - name: Automation Policy - Scope VM Retirement Warning, ResponseExecute Automation
      Model
      description: ! 'Operational: Retirement Warning'
      expression:
      towhat: Vm
      guid: 39621392-2866-11de-af2a-0050568026c2
      created_by:
      updated_by: admin
      notes: This policy raises an automation event when a retirement warning event
        is raised
      active: true
      mode: control
      MiqPolicyContent:
      - qualifier: success
        success_sequence: 1
        failure_synchronous: true
      MiqEvent:
        name: vm_retire_warn
        description: VM Retirement Warning
        guid: 97c85330-fe93-11dd-b5e1-005056903dbc
        event_type: Default
        definition:
        default:
        enabled:
      MiqAction:
        name: raise_automation_event
        description: Raise Automation Event
        guid: e7da3b7a-1139-11e1-9333-005056af009e
        action_type: default
        options: {}
      Condition: []
    - name: Automation Policy - Scope VM Retired Response Execute Automation Model
      description: ! 'Operational: Vm Retired'
      expression:
      towhat: Vm
      guid: 397700ae-2866-11de-af2a-0050568026c2
      created_by:
      updated_by: admin
      notes: This policy raises an automation event when a vm retirement event is
        raised
      active: true

```

```

mode: control
MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  failure_synchronous: true
  MiqEvent:
    name: vm_retired
    description: VM Retired
    guid: e363d8aa-1e1e-11de-8918-0050568005db
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: raise_automation_event
    description: Raise Automation Event
    guid: e7da3b7a-1139-11e1-9333-005056af009e
    action_type: default
    options: {}
  Condition: []
- name: 427a4378-6519-11df-b637-005056a435be
  description: ! 'Analysis: Post Provisioning'
  expression:
  towhat: Vm
  guid: 427a4378-6519-11df-b637-005056a435be
  created_by: admin
  updated_by: admin
  notes: This policy triggers a vm analysis of any newly provisioned VM
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_provisioned
      description: VM Provision Complete
      guid: 2a17a20a-3e8e-11df-9fe2-005056a435be
      event_type: Default
      definition:
      default:
      enabled:
    MiqAction:
      name: vm_analyze
      description: Initiate SmartState Analysis for VM
      guid: 5cbe1082-ce35-11de-a117-005056b0503e
      action_type: default
      options: {}
    Condition: []
- name: 0c2517d8-1ea2-11e0-8e71-005056910000
  description: ! 'Tag: VM Inherit Cluster Location Tag'
  expression:
  towhat: Vm
  guid: 0c2517d8-1ea2-11e0-8e71-005056910000
  created_by: admin
  updated_by: admin
  notes: This policy allows a vm to inherit the location tag of it's parent cluster
    on creation or completion of analysis
  active: true
  mode: control

```

```

MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_create
    description: VM Create Complete
    guid: 4c0b4f12-37c0-11df-b567-005056a40709
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: 60e5d690-1ea2-11e0-8e71-005056910000
    description: ! 'Tag: Inherit Cluster Location Tag'
    guid: 60e5d690-1ea2-11e0-8e71-005056910000
    action_type: inherit_parent_tags
    options:
      :parent_type: ems_cluster
      :cats:
      - location
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_scan_complete
    description: VM Analysis Complete
    guid: f7b8361e-1139-11e1-9333-005056af009e
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: 60e5d690-1ea2-11e0-8e71-005056910000
    description: ! 'Tag: Inherit Cluster Location Tag'
    guid: 60e5d690-1ea2-11e0-8e71-005056910000
    action_type: inherit_parent_tags
    options:
      :parent_type: ems_cluster
      :cats:
      - location
Condition: []
- name: ! 'Do Not Analyze '
  description: ! 'Analysis: Prevent Analysis of Selected VMs'
  expression:
  towhat: Vm
  guid: 3a7959c0-2866-11de-af2a-0050568026c2
  created_by:
  updated_by: admin
  notes: ! 'This policies prevents analysis ofany vm that is tagged as Do Not
    Analyze '
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    failure_synchronous: true
    MiqEvent:
      name: request_vm_scan
      description: VM Analysis Request
      guid: e3292c46-1e1e-11de-8918-0050568005db

```



```

    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: prevent
    description: Prevent current event from proceeding
    guid: d885a118-519b-11e0-8d82-005056af0000
    action_type: default
    options: {}
  Condition:
- name: Do Not Analyze
  description: VM classified as DO_NOT_ANALYZE
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      CONTAINS:
        tag: Vm.managed-exclusions
        value: do_not_analyze
      context_type:
      towhat: Vm
      file_mtime:
      guid: 39ff4444-08e2-11de-829f-005056a164b2
      filename:
      applies_to_exp:
      miq_policy_id: 10000000000001
      notes:
- name: b968f0a0-3d2e-11df-a7e9-005056a40709
  description: ! 'Tag: VM that Requires Analysis'
  expression:
  towhat: Vm
  guid: b968f0a0-3d2e-11df-a7e9-005056a40709
  created_by: admin
  updated_by: admin
  notes:
  active: true
  mode: control
  MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_start
    description: VM Power On
    guid: 404b4630-21a8-11e2-b47a-0050568b19a3
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: a4ccd026-3d2e-11df-a7e9-005056a40709
    description: Tag VM that Requires Analysis
    guid: a4ccd026-3d2e-11df-a7e9-005056a40709
    action_type: tag
    options:
      :tags:
        - /managed/operations/analysis_required
- qualifier: success
  success_sequence: 1
  MiqEvent:

```

```

    name: vm_create
    description: VM Create Complete
    guid: 4c0b4f12-37c0-11df-b567-005056a40709
    event_type: Default
    definition:
      default:
      enabled:
    MiqAction:
      name: a4ccd026-3d2e-11df-a7e9-005056a40709
      description: Tag VM that Requires Analysis
      guid: a4ccd026-3d2e-11df-a7e9-005056a40709
      action_type: tag
      options:
        :tags:
          - /managed/operations/analysis_required
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_reset
    description: VM Reset
    guid: 4c1b8a3a-37c0-11df-b567-005056a40709
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: a4ccd026-3d2e-11df-a7e9-005056a40709
    description: Tag VM that Requires Analysis
    guid: a4ccd026-3d2e-11df-a7e9-005056a40709
    action_type: tag
    options:
      :tags:
        - /managed/operations/analysis_required
  Condition: []
- name: 2f2a1alc-4806-11df-badc-005056a7121f
  description: ! 'Analysis: VM Reconfiguration'
  expression:
  towhat: Vm
  guid: 2f2a1alc-4806-11df-badc-005056a7121f
  created_by: admin
  updated_by: admin
  notes: Performs an analysis on any vm that has been reconfigured
  active: true
  mode: control
  MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_reconfigure
    description: VM Settings Change
    guid: 07367e62-449a-11de-bd4f-005056a83e5d
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: vm_analyze
    description: Initiate SmartState Analysis for VM
    guid: 5cbe1082-ce35-11de-a117-005056b0503e

```

```

        action_type: default
        options: {}
    Condition: []
- name: 0ce6cf38-3d2d-11df-a7e9-005056a40709
  description: ! 'Tag: VM on Successful Analysis'
  expression:
  towhat: Vm
  guid: 0ce6cf38-3d2d-11df-a7e9-005056a40709
  created_by: admin
  updated_by: admin
  notes:
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_scan_complete
      description: VM Analysis Complete
      guid: f7b8361e-1139-11e1-9333-005056af009e
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: cd2f3222-3d2c-11df-a7e9-005056a40709
      description: Tag VM after Successful Analysis
      guid: cd2f3222-3d2c-11df-a7e9-005056a40709
      action_type: tag
      options:
        :tags:
          - /managed/operations/analysis_success
    Condition: []
- name: 07cea762-3d1b-11df-a7e9-005056a40709
  description: ! 'Tag: VM if Analysis not successful'
  expression:
  towhat: Vm
  guid: 07cea762-3d1b-11df-a7e9-005056a40709
  created_by: admin
  updated_by: admin
  notes:
  active: true
  mode: control
  MiqPolicyContent:
  - qualifier: success
    success_sequence: 1
    MiqEvent:
      name: vm_scan_abort
      description: VM Analysis Failure
      guid: 4c48a6fa-37c0-11df-b567-005056a40709
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: fc7f2dde-3d22-11df-a7e9-005056a40709
      description: Tag VM that Fails Analysis
      guid: fc7f2dde-3d22-11df-a7e9-005056a40709
      action_type: tag

```

```
options:  
  :variables:  
    - :value: ''  
      :oid: ''  
      :var_type: <None>  
    - :value: ''  
      :oid: ''  
      :var_type: <None>  
    - :value: ''  
      :oid: ''  
      :var_type: <None>  
    - :value: ''  
      :oid: ''  
      :var_type: <None>  
    - :value: ''  
      :oid: ''  
      :var_type: <None>  
    - :value: ''  
      :oid: ''  
      :var_type: <None>  
    - :value: ''  
      :oid: ''  
      :var_type: <None>  
    - :value: ''  
      :oid: ''  
      :var_type: <None>  
    - :value: ''  
      :oid: ''  
      :var_type: <None>  
    - :value: ''  
      :oid: ''  
      :var_type: <None>  
    - :value: ''  
      :oid: ''  
      :var_type: <None>  
    - :value: ''  
      :oid: ''  
      :var_type: <None>  
    - :value: ''  
      :oid: ''  
      :var_type: <None>  
    - :value: ''  
      :oid: ''  
      :var_type: <None>  
  :tags:  
    - /managed/operations/analysis_failed  
  
Condition: []  
- name: 782068f8-44ee-11e0-99a6-00505688000a  
description: ! 'Analysis: VDI Login'  
expression:  
toward: Vm  
guid: 782068f8-44ee-11e0-99a6-00505688000a  
created_by: admin  
updated_by: admin  
notes: This policy triggers an analysis of a VDI session when a user logs in  
to that session  
active: true  
mode: control  
MiqPolicyContent:  
- qualifier: success  
success_sequence: 1  
MiqEvent:  
name: vm_vdi_login_session  
description: VDI Login Session  
guid: 15fc3cce-448a-11e0-9ad1-00505688000a  
event_type: Default  
definition:  
default:  
enabled:  
MiqAction:  
name: vm_analyze
```

```

        description: Initiate SmartState Analysis for VM
        guid: 5cbel082-ce35-11de-a117-005056b0503e
        action_type: default
        options: {}
    Condition: []
- MiqPolicySet:
    name: fbc1c9bc-53f9-11e0-babf-00505688000a
    description: ! 'Tag Management: Inheritance Policy'
    set_type: MiqPolicySet
    guid: fbc1c9bc-53f9-11e0-babf-00505688000a
    read_only:
    set_data:
        :notes: This policy profile contains policies that enforce Host and VM inheritance
            of parent cluster tags.
    mode: control
    owner_type:
    owner_id:
    MiqPolicy:
    - name: 0c2517d8-1ea2-11e0-8e71-005056910000
      description: ! 'Tag: VM Inherit Cluster Location Tag'
      expression:
      towhat: Vm
      guid: 0c2517d8-1ea2-11e0-8e71-005056910000
      created_by: admin
      updated_by: admin
      notes: This policy allows a vm to inherit the location tag of it's parent cluster
        on creation or completion of analysis
      active: true
      mode: control
      MiqPolicyContent:
      - qualifier: success
        success_sequence: 1
        MiqEvent:
          name: vm_create
          description: VM Create Complete
          guid: 4c0b4f12-37c0-11df-b567-005056a40709
          event_type: Default
          definition:
          default:
          enabled:
        MiqAction:
          name: 60e5d690-1ea2-11e0-8e71-005056910000
          description: ! 'Tag: Inherit Cluster Location Tag'
          guid: 60e5d690-1ea2-11e0-8e71-005056910000
          action_type: inherit_parent_tags
          options:
            :parent_type: ems_cluster
            :cats:
            - location
      - qualifier: success
        success_sequence: 1
        MiqEvent:
          name: vm_scan_complete
          description: VM Analysis Complete
          guid: f7b8361e-1139-11e1-9333-005056af009e
          event_type: Default
          definition:
          default:
          enabled:

```

```

    MiqAction:
      name: 60e5d690-1ea2-11e0-8e71-005056910000
      description: ! 'Tag: Inherit Cluster Location Tag'
      guid: 60e5d690-1ea2-11e0-8e71-005056910000
      action_type: inherit_parent_tags
      options:
        :parent_type: ems_cluster
        :cats:
          - location
    Condition: []
- MiqPolicySet:
  name: bc33dd42-c01d-11e3-b785-001a4a0f459e
  description: VM retirement test
  set_type: MiqPolicySet
  guid: bc33dd42-c01d-11e3-b785-001a4a0f459e
  read_only:
  set_data:
  mode: control
  owner_type:
  owner_id:
  MiqPolicy:
  - name: b218c83c-c01c-11e3-b785-001a4a0f459e
    description: MyNew VM Control Policy
    expression:
    towhat: Vm
    guid: b218c83c-c01c-11e3-b785-001a4a0f459e
    created_by: admin
    updated_by: admin
    notes:
    active: true
    mode: control
    MiqPolicyContent:
    - qualifier: success
      success_sequence: 1
      success_synchronous: true
    MiqEvent:
      name: vm_retired
      description: VM Retired
      guid: e363d8aa-1e1e-11de-8918-0050568005db
      event_type: Default
      definition:
        default:
        enabled:
    MiqAction:
      name: raise_automation_event
      description: Raise Automation Event
      guid: e7da3b7a-1139-11e1-9333-005056af009e
      action_type: default
      options: {}
    Condition: []
- MiqPolicySet:
  name: 4a554d7c-21b4-11e2-a38c-0050568b19a3
  description: VM-Operation Policies
  set_type: MiqPolicySet
  guid: 4a554d7c-21b4-11e2-a38c-0050568b19a3
  read_only:
  set_data:
  mode: control
  owner_type:

```

```

owner_id:
MiqPolicy:
- name: 7408efa8-21b3-11e2-a38c-0050568b19a3
  description: Power-Off Virtual Machines
  expression:
  towhat: Vm
  guid: 7408efa8-21b3-11e2-a38c-0050568b19a3
  created_by: admin
  updated_by: admin
  notes:
  active: true
  mode: control
MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_start
    description: VM Power On
    guid: 404b4630-21a8-11e2-b47a-0050568b19a3
    event_type: Default
    definition:
    default:
    enabled:
  MiqAction:
    name: vm_stop
    description: Stop Virtual Machine
    guid: 37f2da3e-21a8-11e2-b47a-0050568b19a3
    action_type: default
    options: {}
Condition:
- name: d514b2fa-21b3-11e2-a38c-0050568b19a3
  description: VM with Workload Tag Messaging
  modifier: allow
  expression: !ruby/object:MiqExpression
    exp:
      !binary "Q090VEFJTlM=":
      !binary "dGFn": Vm.managed-function
      !binary "dmFsdWU=": messaging
    context_type:
  towhat: Vm
  file_mtime:
  guid: d514b2fa-21b3-11e2-a38c-0050568b19a3
  filename:
  applies_to_exp:
  miq_policy_id:
  notes:
- MiqPolicySet:
  name: 99a57bb8-e15e-11e1-acfa-005056b25af6
  description: poweron
  set_type: MiqPolicySet
  guid: 99a57bb8-e15e-11e1-acfa-005056b25af6
  read_only:
  set_data:
  mode: control
  owner_type:
  owner_id:
  MiqPolicy:
  - name: d4640a18-e15d-11e1-acfa-005056b25af6
    description: powervm

```

```

expression:
towhat: Vm
guid: d4640a18-e15d-11e1-acfa-005056b25af6
created_by: admin
updated_by: admin
notes:
active: true
mode: control
MiqPolicyContent:
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_start
    description: VM Power On
    guid: 404b4630-21a8-11e2-b47a-0050568b19a3
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: b0138b70-e15d-11e1-8744-005056b25af6
    description: powerVM
    guid: b0138b70-e15d-11e1-8744-005056b25af6
    action_type: custom_automation
    options:
      :ae_message: create
      :ae_request: powerVM
- qualifier: success
  success_sequence: 1
  MiqEvent:
    name: vm_poweroff
    description: VM Power Off
    guid: 48beeadc-ae7c-11e1-a76f-005056b25af6
    event_type: Default
    definition:
      default:
      enabled:
  MiqAction:
    name: b0138b70-e15d-11e1-8744-005056b25af6
    description: powerVM
    guid: b0138b70-e15d-11e1-8744-005056b25af6
    action_type: custom_automation
    options:
      :ae_message: create
      :ae_request: powerVM
Condition: []

```

### 3.18.3 Alerts.yaml

Link: [Alerts.yaml](#)

Source:

```

---
- MiqAlert:
  guid: d59185a4-40bc-11de-bd12-005056a170fa
  description: CPU Ready > 4000 ms for more than 10 min
  options:

```



```

      :notifications:
      :email:
      :from: ''
      :to:
      - alert@manageiq.com
db: Vm
expression:
  :mode: internal
  :eval_method: realtime_performance
  :options:
    :operator: ! '>'
    :perf_column: cpu_ready_delta_summation
    :value_threshold: '4000'
    :rt_time_threshold: 600
  responds_to_events: vm_perf_complete
  enabled:
- MiqAlert:
  guid: 20d93374-fde1-11e1-a360-005056b25af6
  description: CPU Usage > 50
  options:
    :notifications:
      :delay_next_evaluation: 600
      :evm_event: {}
      :automate:
        :event_name: alert_cpu
db: Vm
expression:
  :eval_method: realtime_performance
  :mode: internal
  :options:
    :perf_column: cpu_usage_rate_average
    :operator: ! '>'
    :value_threshold: '50'
    :trend_direction: none
    :trend_steepness:
    :debug_trace: 'false'
    :rt_time_threshold: 60
  responds_to_events: vm_perf_complete
  enabled: true
- MiqAlert:
  guid: 5bfdef56-13d2-11e2-a735-005056b057a8
  description: CPU Usage Exceeds 90% For More Than 1 Min
  options:
    :notifications:
      :delay_next_evaluation: 600
    :snmp:
      :host:
      - 192.168.255.26
      :trap_id: 1.3.6.1.4.1.33482.3
      :snmp_version: v2
      :variables:
      - :oid: description
        :var_type: OctetString
        :value: Virtual Machine
      - :oid: category
        :var_type: OctetString
        :value: Perfomance
      - :oid: Message
        :var_type: OctetString

```

```

      :value: ${cause.description}
    - :oid: object
      :var_type: OctetString
      :value: Name:${object.name}
    - :oid: location
      :var_type: OctetString
      :value: Datastore:${object.path}
    - :oid: platform
      :var_type: OctetString
      :value: OS:${object.platform}
    - :oid: url
      :var_type: OctetString
      :value: http://10.10.1.200/VM/${object.id}
    - :oid: source
      :var_type: OctetString
      :value: EVM:${object.ems}
    - :oid: custom1
      :var_type: OctetString
      :value: Created:${object.created_on} Retires:${retires_on}
    - :oid: custom2
      :var_type: OctetString
      :value: ! 'Cluster:${object.ems_cluster_name} Host: ${object.host_name}'
db: Vm
expression:
  :eval_method: realtime_performance
  :mode: internal
  :options:
    :value_threshold: '90'
    :perf_column: v_pct_cpu_used_delta_summation
    :trend_steepness:
    :rt_time_threshold: 60
    :trend_direction: none
    :operator: ! '>'
    :debug_trace: 'false'
  responds_to_events: vm_perf_complete
  enabled: true
- MiqAlert:
  guid: 59174666-cfed-11e2-a54c-000c2980bea6
  description: CloudFLEX
  options:
    :notifications:
      :delay_next_evaluation: 120
      :evm_event: {}
      :automate:
        :event_name: CloudFLEX_EVENT
db: Vm
expression:
  :eval_method: realtime_performance
  :mode: !binary |-
    aW50ZXJuYWw=
  :options:
    :perf_column: v_pct_cpu_used_delta_summation
    :operator: !binary |-
      Pg==
    :value_threshold: '50'
    :trend_direction: !binary |-
      bm9uZQ==
    :trend_steepness:
    :debug_trace: !binary |-

```

```

      ZmFsc2U=
      :rt_time_threshold: 120
      responds_to_events: vm_perf_complete
      enabled: true
- MiqAlert:
  guid: eb88f942-c23e-11de-a3be-000c290de4f9
  description: Cluster DRS not enabled
  options:
    :notifications:
      :email:
        :from: ''
        :to:
          - alert@manageiq.com
  db: EmsCluster
  expression: !ruby/object:MiqExpression
  exp:
    =:
      value: 'false'
      field: EmsCluster-drs_enabled
  responds_to_events:
    enabled:
- MiqAlert:
  guid: 196868de-c23f-11de-a3be-000c290de4f9
  description: Cluster HA not enabled
  options:
    :notifications:
      :email:
        :from: ''
        :to:
          - alert@manageiq.com
  db: EmsCluster
  expression: !ruby/object:MiqExpression
  exp:
    =:
      value: 'false'
      field: EmsCluster-ha_enabled
  responds_to_events:
    enabled:
- MiqAlert:
  guid: 82f853b0-bf36-11de-b3b4-000c290de4f9
  description: Datacenter VMs > 10
  options:
    :notifications:
      :email:
        :from: ''
        :to:
          - alert@manageiq.com
  db: Storage
  expression: !ruby/object:MiqExpression
  exp:
    ! '>':
      value: 10
      field: Storage-v_total_vms
  responds_to_events:
    enabled:
- MiqAlert:
  guid: 655ccda-6ae5-11e0-bdef-005056a461b8
  description: Datastore Free Space <= 10%
  options:

```

```

:notifications:
  :snmp:
    :variables:
      - :value: ! 'MIQ Datatstore Alert: DEMO'
        :oid: category
        :var_type: OctetString
      - :value: Datastore Free Space <= 10%
        :oid: message
        :var_type: OctetString
    :host:
      - 204.130.60.75
    :trap_id: critical
    :snmp_version: v2
  :delay_next_evaluation: 86400
  :email:
    :from: ''
    :to:
      - cloud_ops@miq.net
  :evm_event: {}
db: Storage
expression: !ruby/object:MiqExpression
exp:
  <=:
    value: '10'
    field: Storage-v_free_space_percent_of_total
  context_type:
  responds_to_events: _hourly_timer_
  enabled: true
- MiqAlert:
  guid: f0782622-fa6c-11e0-98ad-005056be005b
  description: EVM Server High App Disk Usage
  options:
    :notifications:
      :delay_next_evaluation: 14400
      :evm_event: {}
  db: MiqServer
  expression:
    :mode: internal
    :eval_method: nothing
    :options: {}
  responds_to_events: evm_server_app_disk_high_usage
  enabled: true
- MiqAlert:
  guid: 50b6ae6e-fa6d-11e0-a117-005056be005b
  description: EVM Server High DB Disk Usage
  options:
    :notifications:
      :delay_next_evaluation: 14400
      :evm_event: {}
  db: MiqServer
  expression:
    :mode: internal
    :eval_method: nothing
    :options: {}
  responds_to_events: evm_server_db_disk_high_usage
  enabled: true
- MiqAlert:
  guid: 6f0f695a-fa6d-11e0-a117-005056be005b
  description: EVM Server High Log Disk Usage

```

```

    options:
      :notifications:
        :delay_next_evaluation: 14400
        :evm_event: {}
    db: MiqServer
    expression:
      :mode: internal
      :eval_method: nothing
      :options: {}
    responds_to_events: evm_server_log_disk_high_usage
    enabled: true
- MiqAlert:
  guid: 8ef83828-fa6d-11e0-98ad-005056be005b
  description: EVM Server High System Disk Usage
  options:
    :notifications:
      :delay_next_evaluation: 14400
      :evm_event: {}
  db: MiqServer
  expression:
    :mode: internal
    :eval_method: nothing
    :options: {}
  responds_to_events: evm_server_system_disk_high_usage
  enabled: true
- MiqAlert:
  guid: 3bfdde58-fa6c-11e0-a117-005056be005b
  description: EVM Server Not Responding
  options:
    :notifications:
      :delay_next_evaluation: 14400
      :evm_event: {}
  db: MiqServer
  expression:
    :mode: internal
    :eval_method: nothing
    :options: {}
  responds_to_events: evm_server_not_responding
  enabled: true
- MiqAlert:
  guid: cdf91470-fa6d-11e0-a117-005056be005b
  description: EVM Server Started
  options:
    :notifications:
      :delay_next_evaluation: 14400
      :evm_event: {}
  db: MiqServer
  expression:
    :mode: internal
    :eval_method: nothing
    :options: {}
  responds_to_events: evm_server_start
  enabled: true
- MiqAlert:
  guid: fc2ae066-44b8-11de-900a-005056a170fa
  description: Host Event Log Error - Failed to validate VM IP address
  options:
    :notifications:
      :email:

```

```

      :from: ''
      :to:
      - alert@manageiq.com
db: Host
expression:
  :mode: internal
  :eval_method: hostd_log_threshold
  :options:
    :event_log_message_filter_type: INCLUDES
    :event_log_source: VmMisc
    :freq_threshold: '2'
    :event_log_message_filter_value: Failed to validate VM IP address
    :time_threshold: 86400
  responds_to_events: host_scan_complete
  enabled:
- MiqAlert:
  guid: 0bd6ac74-fa70-11e0-a117-005056be005b
  description: Host Credentials Authentication Error
  options:
    :notifications:
      :delay_next_evaluation: 14400
      :evm_event: {}
  db: Host
  expression:
    :mode: internal
    :eval_method: nothing
    :options: {}
  responds_to_events: host_auth_error
  enabled: true
- MiqAlert:
  guid: 3599fa6e-f9d7-11e0-a117-005056be005b
  description: Host Credentials are Invalid
  options:
    :notifications:
      :delay_next_evaluation: 14400
      :evm_event: {}
  db: Host
  expression:
    :mode: internal
    :eval_method: nothing
    :options: {}
  responds_to_events: host_auth_invalid
  enabled: true
- MiqAlert:
  guid: 9bc0d572-40bd-11de-bd12-005056a170fa
  description: Host Datastore < 5% of Free Space
  options:
    :notifications:
      :email:
        :from: ''
        :to:
        - alert@manageiq.com
  db: Host
  expression: !ruby/object:MiqExpression
  exp:
    FIND:
      checkany:
        ! '>':
          value: 95

```

```

        field: Host.storages-v_used_space_percent_of_total
      search:
        IS NOT NULL:
          field: Host.storages-name
      responds_to_events:
        enabled:
- MiqAlert:
  guid: 8a6d32a8-44b8-11de-900a-005056a170fa
  description: ! 'Host Event Log Error - Memory Exceed Soft Limit '
  options:
    :notifications:
      :email:
        :from: ''
        :to:
          - alert@manageiq.com
  db: Host
  expression:
    :mode: internal
    :eval_method: hostd_log_threshold
    :options:
      :event_log_message_filter_type: INCLUDES
      :event_log_source: Memory checker
      :freq_threshold: '2'
      :event_log_message_filter_value: exceeds soft limit
      :event_log_level: warn
      :time_threshold: 86400
  responds_to_events: host_scan_complete
  enabled:
- MiqAlert:
  guid: 561d023c-bf36-11de-b3b4-000c290de4f9
  description: Host VMs >10
  options:
    :notifications:
      :email:
        :from: ''
        :to:
          - alert@manageiq.com
  db: Host
  expression: !ruby/object:MiqExpression
  exp:
    ! '>':
      value: 10
      field: Host-v_total_vms
  responds_to_events:
  enabled:
- MiqAlert:
  guid: a6c34cee-94f3-11df-92e9-0050569a006f
  description: Max - Allocated RAM per VM
  options:
    :notifications:
      :delay_next_evaluation: 3600
      :evm_event: {}
  db: Vm
  expression: !ruby/object:MiqExpression
  exp:
    ! '>':
      value: '255'
      field: Vm-mem_cpu
  context_type:

```

```
  responds_to_events: vm_discover
  enabled: true
- MiqAlert:
  guid: ddfd7df4-950e-11df-b1e3-0050568a6293
  description: Max - Hosts per Cluster
  options:
    :notifications:
      :delay_next_evaluation: 3600
      :evm_event: {}
  db: EmsCluster
  expression: !ruby/object:MiqExpression
    exp:
      ! '>':
        count: EmsCluster.hosts
        value: '32'
      context_type:
        responds_to_events: host_connect
        enabled: true
- MiqAlert:
  guid: 7129b8d8-978d-11df-8cd7-0050569a4433
  description: Max - vCPU per Core >20
  options:
    :notifications:
      :delay_next_evaluation: 3600
      :evm_event: {}
  db: Host
  expression: !ruby/object:MiqExpression
    exp:
      ! '>':
        value: '20'
        field: Host.ems_cluster-v_cpu_vr_ratio
      context_type:
        responds_to_events: host_connect
        enabled: true
- MiqAlert:
  guid: 2f4e5e06-94f3-11df-92e9-0050569a006f
  description: Max - vCpus per VM
  options:
    :notifications:
      :delay_next_evaluation: 3600
      :evm_event: {}
  db: Vm
  expression: !ruby/object:MiqExpression
    exp:
      ! '>':
        value: '8'
        field: Vm.hardware-numvcpus
      context_type:
        responds_to_events: vm_discover
        enabled: true
- MiqAlert:
  guid: dab5b816-f789-11e1-9144-005056b25af6
  description: Test - VM Analysis Complete
  options:
    :notifications:
      :delay_next_evaluation: 300
      :email:
        :to:
          - scottfisher1@gmail.com
```



```

      :evm_event: {}
db: Vm
expression:
  :eval_method: nothing
  :mode: internal
  :options: {}
  responds_to_events: vm_scan_complete
  enabled: true
- MiqAlert:
  guid: 391d87fc-fa70-11e0-98ad-005056be005b
  description: VC Authentication Error
  options:
    :notifications:
      :delay_next_evaluation: 14400
      :evm_event: {}
  db: ExtManagementSystem
  expression:
    :mode: internal
    :eval_method: nothing
    :options: {}
  responds_to_events: ems_auth_error
  enabled: true
- MiqAlert:
  guid: 576aabca-f9d7-11e0-a117-005056be005b
  description: VC Credentials are Invalid
  options:
    :notifications:
      :delay_next_evaluation: 14400
      :evm_event: {}
  db: ExtManagementSystem
  expression:
    :mode: internal
    :eval_method: nothing
    :options: {}
  responds_to_events: ems_auth_invalid
  enabled: true
- MiqAlert:
  guid: 58e8a372-bff9-11de-b3b4-000c290de4f9
  description: VM CD Drive or Floppy Connected
  options:
    :notifications:
      :email:
        :from: ''
        :to:
          - alert@manageiq.com
  db: Vm
  expression: !ruby/object:MiqExpression
  exp:
    or:
      - FIND:
        checkall:
          STARTS WITH:
            value: 'true'
            field: Vm.hardware.disks-start_connected
        search:
          INCLUDES:
            value: cdrom
            field: Vm.hardware.disks-device_type
      - FIND:

```

```

      checkall:
        INCLUDES:
          value: 'true'
          field: Vm.hardware.disks-start_connected
      search:
        INCLUDES:
          value: floppy
          field: Vm.hardware.disks-device_type
      responds_to_events:
        enabled:
- MiqAlert:
  guid: ce2f8846-44a5-11de-b543-005056a170fa
  description: VM CPU count was decreased
  options:
    :notifications:
      :email:
        :from: ''
        :to:
          - alert@manageiq.com
  db: Vm
  expression:
    :mode: internal
    :eval_method: reconfigured_hardware_value
    :options:
      :operator: Decreased
      :hdw_attr: :numvcpus
  responds_to_events: vm_reconfigure
  enabled:
- MiqAlert:
  guid: c2fc477a-44a5-11de-b543-005056a170fa
  description: VM CPU count was increased
  options:
    :notifications:
      :email:
        :from: ''
        :to:
          - alert@manageiq.com
  db: Vm
  expression:
    :mode: internal
    :eval_method: reconfigured_hardware_value
    :options:
      :operator: Increased
      :hdw_attr: :numvcpus
  responds_to_events: vm_reconfigure
  enabled:
- MiqAlert:
  guid: 4077943a-c240-11de-a3be-000c290de4f9
  description: VM Environment Tag <> Datastore Environment Tag
  options:
    :notifications:
      :email:
        :from: ''
        :to:
          - alert@manageiq.com
  db: Vm
  expression: !ruby/object:MiqExpression
  exp:
    and:

```

```

- CONTAINS:
  tag: Vm.managed-environment
  value: prod
- not:
  CONTAINS:
    tag: Vm.storage.managed-environment
    value: prod
responds_to_events:
enabled:
- MiqAlert:
  guid: 89db0be8-c240-11de-a3be-000c290de4f9
  description: VM Environment Tag <> Host Environment Tag
  options:
    :notifications:
      :email:
      :from: ''
      :to:
        - alert@manageiq.com
  db: Vm
  expression: !ruby/object:MiqExpression
  exp:
    and:
      - CONTAINS:
          tag: Vm.managed-environment
          value: prod
      - not:
          CONTAINS:
            tag: Vm.host.managed-environment
            value: prod
    responds_to_events:
    enabled:
- MiqAlert:
  guid: 731da3b2-40bc-11de-bd12-005056a170fa
  description: ! 'VM Guest C: Drive < 10% Free'
  options:
    :notifications:
      :email:
      :from: ''
      :to:
        - alert@manageiq.com
  db: Vm
  expression: !ruby/object:MiqExpression
  exp:
    and:
      - =:
          value: windows
          field: Vm-platform
      - FIND:
          checkall:
            <:
              value: 10
              field: Vm.hardware.volumes-free_space_percent
          search:
            =:
              value: ! 'C:'
              field: Vm.hardware.volumes-name
    responds_to_events:
    enabled:
- MiqAlert:

```

```

guid: 1bb81254-44a6-11de-b543-005056a170fa
description: VM Guest Windows Event Log Error - NtpClient
options:
  :notifications:
    :email:
      :from: ''
      :to:
        - alert@manageiq.com
db: Vm
expression:
  :mode: internal
  :eval_method: event_log_threshold
  :options:
    :event_log_message_filter_type: INCLUDES
    :freq_threshold: '1'
    :event_log_message_filter_value: NtpClient
    :event_log_level: error
    :time_threshold: 86400
  responds_to_events: vm_scan_complete
  enabled:
- MiqAlert:
  guid: f8b870d0-c23d-11de-a3be-000c290de4f9
  description: VM Memory Balloon > 250 in last 10 min
  options:
    :notifications:
      :email:
        :from: ''
        :to:
          - alert@manageiq.com
  db: Vm
  expression:
    :mode: internal
    :eval_method: realtime_performance
    :options:
      :operator: ! '>'
      :perf_column: mem_vmmemctl_absolute_average
      :value_threshold: '250'
      :rt_time_threshold: 600
    responds_to_events: vm_perf_complete
    enabled:
- MiqAlert:
  guid: fbe4b5ee-447e-11de-aaba-005056a170fa
  description: VM Memory was decreased
  options:
    :notifications:
      :email:
        :from: ''
        :to:
          - alert@manageiq.com
  db: Vm
  expression:
    :mode: internal
    :eval_method: reconfigured_hardware_value
    :options:
      :operator: Decreased
      :hdw_attr: memory_cpu
    responds_to_events: vm_reconfigure
    enabled:
- MiqAlert:

```

```

guid: e750cdcc-447c-11de-aaba-005056a170fa
description: VM Memory was increased
options:
  :notifications:
    :email:
      :from: ''
      :to:
        - alert@manageiq.com
db: Vm
expression:
  :mode: internal
  :eval_method: reconfigured_hardware_value
  :options:
    :operator: Increased
    :hdw_attr: memory_cpu
  responds_to_events: vm_reconfigure
  enabled:
- MiqAlert:
  guid: 3cfbb5ce-40be-11de-bd12-005056a170fa
  description: VM Migration > 1 in last 30 min
  options:
    :notifications:
      :email:
        :from: ''
        :to:
          - alert@manageiq.com
  db: Vm
  expression:
    :mode: internal
    :eval_method: event_threshold
    :options:
      :event_types:
        - RelocateVM_Task_Complete
      :freq_threshold: '2'
      :time_threshold: 1800
    responds_to_events: ! '["RelocateVM_Task_Complete"]'
    enabled:
- MiqAlert:
  guid: fb73af80-40bd-11de-bd12-005056a170fa
  description: VM Power On > 2 in last 15 min
  options:
    :notifications:
      :email:
        :from: ''
        :to:
          - alert@manageiq.com
  db: Vm
  expression:
    :mode: internal
    :eval_method: event_threshold
    :options:
      :event_types:
        - PowerOnVM_Task_Complete
      :freq_threshold: '2'
      :time_threshold: 900
    responds_to_events: ! '["PowerOnVM_Task_Complete"]'
    enabled:
- MiqAlert:
  guid: fdee2784-bf2c-11de-b3b4-000c290de4f9

```

```

description: VM Silver and CPU > 1
options:
  :notifications:
    :email:
      :from: ''
      :to:
        - alert@manageiq.com
db: Vm
expression: !ruby/object:MiqExpression
exp:
  and:
    - CONTAINS:
      tag: Vm.managed-service_level
      value: silver
    - ! '>':
      value: 1
      field: Vm.hardware-numvcpus
responds_to_events:
  enabled:
- MiqAlert:
  guid: 9b61fd9e-bf35-11de-b3b4-000c290de4f9
  description: VM Silver and RAM > 2 GB
  options:
    :notifications:
      :email:
        :from: ''
        :to:
          - alert@manageiq.com
db: Vm
expression: !ruby/object:MiqExpression
exp:
  and:
    - CONTAINS:
      tag: Vm.managed-service_level
      value: silver
    - ! '>':
      value: 2048
      field: Vm.hardware-memory_cpu
responds_to_events:
  enabled:
- MiqAlert:
  guid: 5cd2b880-be53-11de-8d65-000c290de4f9
  description: VM Unregistered
  options:
    :notifications:
      :email:
        :from: ''
        :to:
          - alert@manageiq.com
db: Vm
expression: !ruby/object:MiqExpression
exp:
  and:
    - IS EMPTY:
      value: ''
      field: Vm.host-name
    - IS NOT EMPTY:
      field: Vm.storage-name
responds_to_events:

```

```

  enabled:
- MiqAlert:
  guid: a9532172-44a5-11de-b543-005056a170fa
  description: VM VMotion > 1 in last 30 min
  options:
    :notifications:
      :email:
      :from: ''
      :to:
        - alert@manageiq.com
  db: Vm
  expression:
    :mode: internal
    :eval_method: event_threshold
    :options:
      :event_types:
        - MigrateVM_Task
      :freq_threshold: '1'
      :time_threshold: 1800
  responds_to_events: ! ["MigrateVM_Task"]'
  enabled:
- MiqAlert:
  guid: 5709f346-05a5-11e1-9288-005056880000
  description: VM with CPU Ready > 2% for 2mins
  options:
    :notifications:
      :delay_next_evaluation: 600
    :automate:
      :event_name: VM_Alert_CPU_Ready
      :evm_event: {}
  db: Vm
  expression:
    :mode: internal
    :eval_method: realtime_performance
    :options:
      :trend_direction: none
      :operator: ! '>'
      :value_threshold: '2'
      :perf_column: v_pct_cpu_ready_delta_summation
      :debug_trace: 'false'
      :trend_steepness:
      :rt_time_threshold: 120
  responds_to_events: vm_perf_complete
  enabled: true
- MiqAlert:
  guid: 8261bf0a-be54-11de-8d65-000c290de4f9
  description: VMs on local storage
  options:
    :notifications:
      :email:
      :from: ''
      :to:
        - alert@manageiq.com
  db: Storage
  expression: !ruby/object:MiqExpression
  exp:
    ! '!=':
      value: 1
      field: Storage-v_total_hosts

```

```
responds_to_events:
enabled:
```

### 3.19 Database Backup Procedure

There are two way to perform backups.

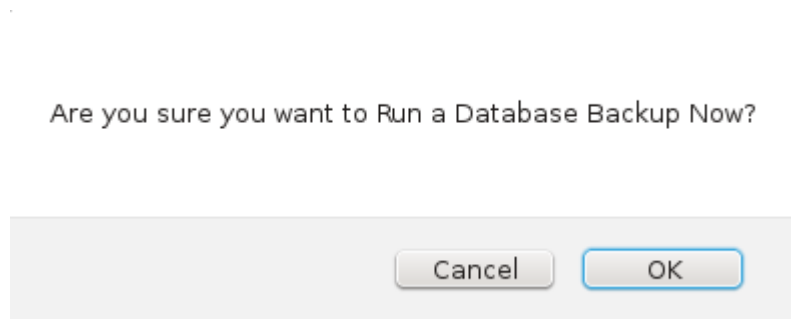
- 1) RECOMMENDED: This method is done through the Web UI and allows you to set up schedules and to have the backups be on an NFS or Samba share.
- 2) Manually through the DB Appliance SSH session

#### 3.19.1 Web UI: Single Run Database Backup

- Go to Configure > Configuration > Diagnostics (Left hand navigation menu) > Select Region (i.e. Region 10) > Click on Database Tab
- in the Database Backup Settings enter the following:

Type:	Network File System
URI: nfs://	c3pudrnas1:/drnas/cloudforms

- Click on Submit
- Click OK in the pop-up "Are you sure you want to Run a Database Backup Now?"



#### 3.19.2 Web UI: Scheduled Database Backup

- Go to Configure > Configuration > Settings > Select Schedules within the Left Hand Menu

../cloudforms/database/menu.png

- Fill out the settings as show in the image



Basic Information	
Name	Database Backup
Description	Database Backup
Active	<input checked="" type="checkbox"/>
Action	Database Backup ▼

Database Backup Settings	
Type	Network File System ▼
URI	nfs:// c3pudrnas1:/drnas/cloudforms

Timer	
Run	Daily ▼ every Day ▼
Time Zone	(GMT-05:00) Eastern Time (US & Canada) ▼ * Changing the Time Zone will reset the Starting Date and Time fields below
Starting Date	07/11/2014
Starting Time (EDT)	22 ▼ h 0 ▼ m

- Click Add

### 3.19.3 SSH: Manual Database Backup

- SSH into the appliance
- switch to postgres user

```
su - postgres
```

- Run backup command

```
pg_dump vmdb_production | gzip > /tmp/postgres_db_backup.gz
```

- To restore

```
cat /tmp/postgres_db_backup.gz | gunzip | psql vmdb_production
```

## 3.20 Member Groups

### 3.20.1 Creating/Importing Group from LDAP/Active Directory

- Go to Configure > Configuration > Access Control > Click on Groups
- Click on the Configuration Button > Select Add New Group
- In the Group Information enter the following:

Description:	<Name of LDAP Group>
Role:	<Select appropriate Role that was created>

- Select Filters for this group on the right.
- Click on Save



#### Important

The filters selected is what will determine what objects the user in this group will be able to see. Example: If the user is part of Department A, and you select "Department > Department A" this user will only EVER see any objects that are tagged with the "Department A" tag.

Example:

Adding a new Group

**Group Information**

Description: Department A ☒ (Look Up LDAP Groups)

Role: Premier-Developer

**LDAP Group Look Up**

User to Look Up:

User Id:

Password:

**Assign Filters**

Premier, Inc Tags | Hosts & Clusters | VMs & Templates

This user is limited to items with the selected tags.

- Auto Approve - Max CPU
- Auto Approve - Max Memory
- Auto Approve - Max Retirement Days
- Auto Approve - Max VM
- Cost Center
- Department
  - ☒ Database Team
  - ☒ **Department A**
  - ☐ Department B
  - ☐ Department C
  - ☐ Engineering
  - ☐ Financial Services
  - ☐ Human Resources

#### Note

You may also leave the Description Blank and then check the "(Look Up LDAP Groups)" check-box and in the "LDAP Group Look Up" section enter a User to Look up and use your LDAP user / password to retrieve all of the groups this member is a part of. Then select from the Drop Down in "Group Information" with the according LDAP/AD Group that you want to create. Once the group is select it will automatically replace the contents of the "Description" Field. After this is done, select the according Filters on the right side.

### 3.20.2 Adding Smart Management Tag to Group



- Select the Group that was previously created
- Click on Policy
- Click on "Edit Premier, Inc's Tags for this Group"
- in the "Select a customer tag to assign" select Department, then select the appropriate Department
- in the "Select a customer tag to assign" select Cost Center, then select the appropriate Cost Center

Example:

Tag Assignment

Select a customer tag to assign: Cost Center \*

<Select a value to assign>

	Category	Assigned Value
	Cost Center *	Unix Team
	Department	Unix Team

\* Only a single value can be assigned from these categories

- Click Save

### 3.20.3 Groups created during Engagement

Group Name	Role	Tag: Cost Center	Tag: Department	Filters	Notes
Unix Admins	Premier-Admin	Unix Team	Unix Team	None	No Tags or Filters are created in order to assure the admins can see ALL resources
ITS Unix Admins	Premier-Admin	Unix Team	Unix Team	None	No Tags or Filters are created in order to assure the admins can see ALL resources
ITS Server Team	Premier-Developer	Department A	Department A	Department A	This will only allow this group to view only objects/resources tagged with Department A

- NOTE: The Smart Management Tags added to groups will make it so that when these users in these groups provision any Instances/VM's it will automatically tag the Instances/VM's with the provided tags

## 3.21 Tag Taxonomy

### 3.21.1 Environment

Name	Display
dev	Development

Name	Display
preprod	PreProd
prod	Production
qa	QA
test	Test

### 3.21.2 Locations

Name	Display
kansas_city	Kansas City

### 3.21.3 Owners

Name	Display
developers	Developers
engineer	Engineer
unixteam	Unix Team
windowsteam	Windows Team

### 3.21.4 Provisioning Scope

Name	Display
all	All

---

#### Note

Additional Provisioning Scopes to be added at a later time

---

### 3.21.5 Storage Types

Name	Display
tier1	Tier 1
tier2	Tier 2
tier3	Tier 3

### 3.21.6 Cost Center

Name	Display
database_team	Database Team
department_a	Department A
department_b	Department B
department_c	Department C
engineering	Engineering
finance	Financial Services
hr	Human Resources
infrastructure	Infrastructure

Name	Display
marketing	Marketing
network_team	Network Team
unix_team	Unix Team
windows_team	Windows Team

---

**Note**

Additional Cost Center to be added at a later time

---

### 3.21.7 Department

Name	Display
database_team	Database Team
department_a	Department A
department_b	Department B
department_c	Department C
engineering	Engineering
finance	Financial Services
hr	Human Resources
infrastructure	Infrastructure
marketing	Marketing
network_team	Network Team
unix_team	Unix Team
windows_team	Windows Team

---

**Note**

Additional Departments to be added at a later time

---

### 3.21.8 Workload

Name	Display
active_directory	Active Directory Server
application_servers	Application Servers
cognos	Cognos
database	Database
db2_server	IBM DB2
desktop	Desktop
dhcp	DHCP Server
evm_appliance	EVM Appliance
hadoop	Hadoop
infrastructure	Virtual Infrastructure Management
jboss_server	JBOSS Server
messaging	Messaging
oracle_server	Oracle Database
proxy_server	Proxy Server
security	Security

Name	Display
web_server	Web Server
websphere_server	Websphere

---

**Note**

Additional Cost Center to be added at a later time

---

**3.21.9 Service Level**

Name	Display
gold	Gold
platinum	Platinum
silver	Silver

**3.21.10 Auto Approve - Max CPU**

Name	Display
1	1
2	2
3	3
4	4
5	5

**3.21.11 Auto Approve - Max Memory**

Name	Display
1024	1GB
2048	2GB
4096	4GB
8192	8GB

**3.21.12 Auto Approve - Retirement Days**

Name	Display
30	30
60	60
90	90
180	180

**3.21.13 Auto Approve - Max VM**

Name	Display
1	1
2	2
3	3
4	4

Name	Display
5	5

### 3.21.14 Quota - Max Memory

Name	Display
1024	1GB
2048	2GB
4096	4GB
8192	8GB
10240	10GB
16384	16GB

### 3.21.15 Quota - Max Storage

Name	Display
10	10GB
20	20GB
40	40GB
80	80GB
100	100GB
200	200GB
400	400GB
1000	1TB

### 3.21.16 Quota - Max CPU

Name	Display
1	1
2	2
3	3
4	4
5	5
10	10
20	20
30	30

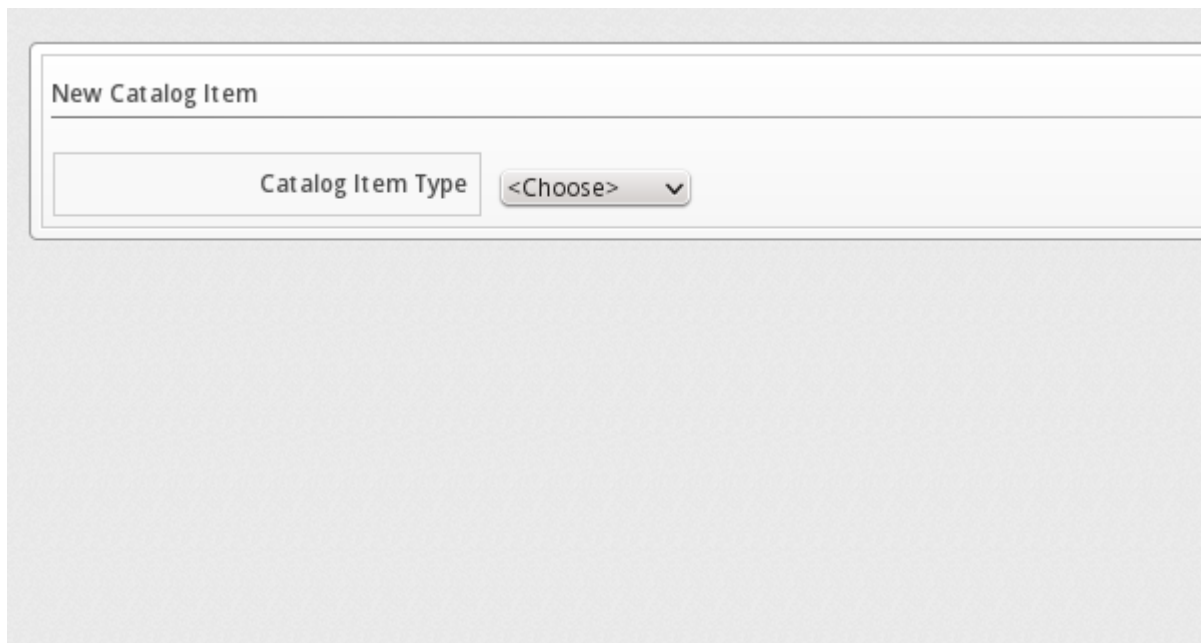
## 3.22 Service Catalog

### 3.22.1 Create new Catalogs

- Go to Services > Catalog > Click on "Catalogs" menu on the left hand side
- Click the "Configuration" Button
- Select "Add a New Catalog"
- Enter the Name of the Catalog
- Enter the Description of the Catalog

### 3.22.2 Create New Catalog Item

- Go to Services > Catalog > Click on "Catalog Items" menu on the left hand side
- Select the Catalog that was previously created
- Click the "Configuration" Button
- Select "Add a New Catalog Item"
- Should bring you to the "Basic Info" Tab
  - Choose the Catalog Item Type, i.e. Openstack



New Catalog Item

Catalog Item Type <Choose> v

- Enter the Name and Description and Check the "Display in Catalog"



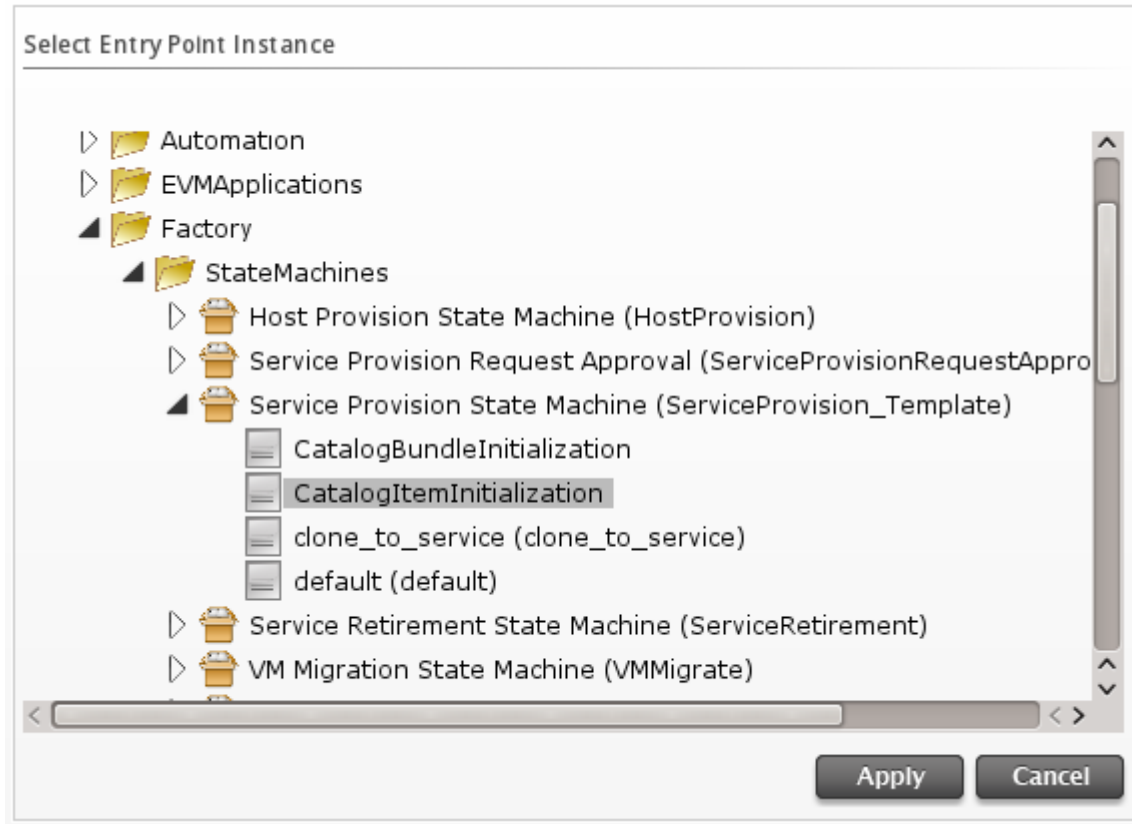
Basic Info Details Request Info

Basic Info

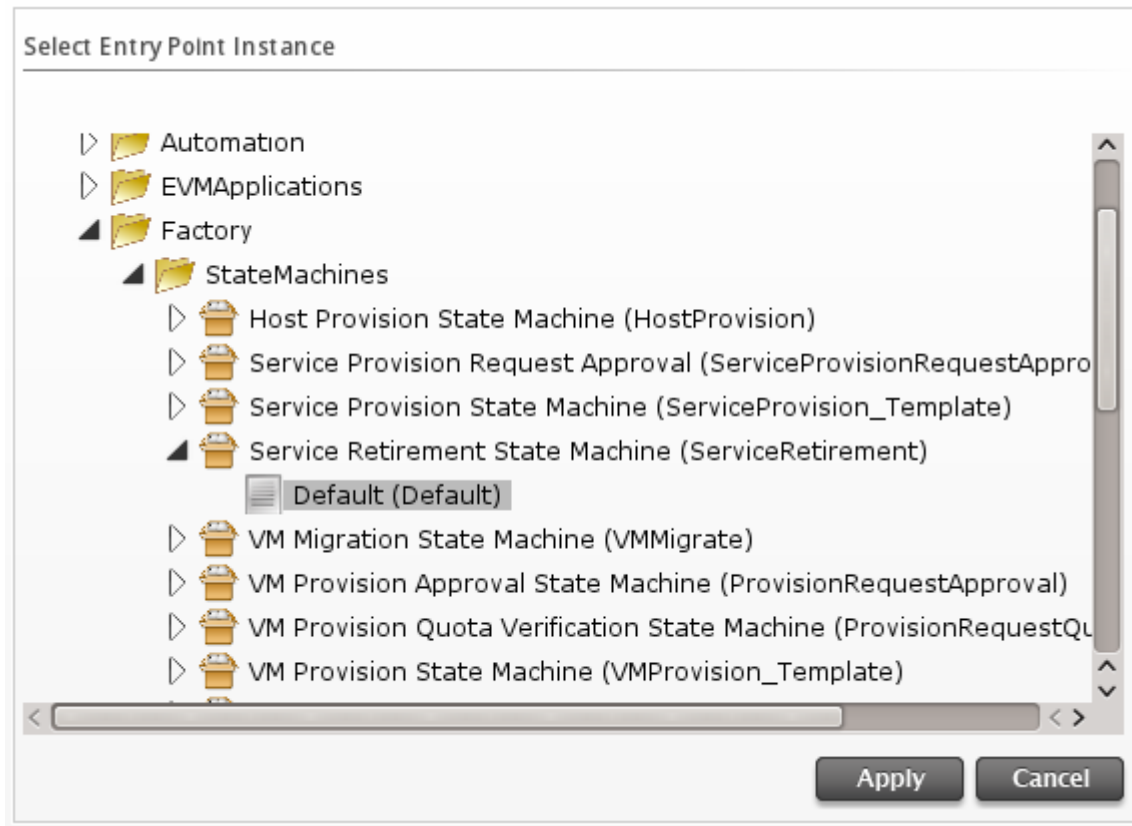
Name / Description RHEL 6.4 - Medium / RHEL 6.4 - Medium ☒ Display in Catalog

- Once the rest of the view is expanded Select the Catalog. i.e. 001-Dev
- Select the Dialog i.e. Basic VM
- Provisioning Entry Point (NS/CIs/Inst): /Factory/StateMachines/ServiceProvision\_Template/CatalogItemInitialization

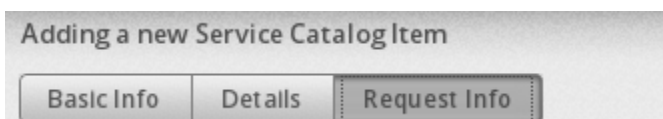




- Click Apply
- Retirement Entry Point (NS/CIs/Inst): /Factory/StateMachines/ServiceRetirement/Default



- Click Apply
  - Click on the "Request Info" Tab



- Request Info: Catalog
  - Select Name of the Template (i.e. rhel6)
  - Enter Instance Name "changeme" (note: this will be changed later using the Service Dialog, just leave it as changeme)

Request Info

Catalog

Environment

Properties

Customize

Schedule

Select

Name \*

Name ▲	Operating System	Platform	C
<None>			
cirros		unknown	0
rhel6		linux	0

Naming

Instance Name \*

changeme

- Request Info: Click on the Environment Tab
  - Placement Options: Availability Zones: **nova**
  - Placement Options: Cloud Network: **publicnet**

**Request Info**

Catalog Environment **Properties** Customize Schedule

---

**Placement**

Choose Automatically ☐

**Placement - Options**

Availability Zones	nova ▾
Cloud Network	publicnet ▾
Security Groups	<None> default: default
Public IP Address	<No Choices Available> ▾

- Request Info: Click on the Properties Tab
  - Properties: Instance Type: i.e. m1.medium
  - Properties: Guest Access Key Pair: devops

**Request Info**

Catalog Environment **Properties** Customize Schedule

---

**Properties**

Instance Type *	m1.medium ▾
Guest Access Key Pair	devops ▾

- Request Info: Click on the Schedule Tab
  - Schedule: Time until Retirement: i.e. Indefinite

**Request Info**

Catalog Environment Properties Customize **Schedule**

---

**Lifespan**

**Time until Retirement** Indefinite ▼

Fields marked with \* are required.

- Click Add

### 3.22.3 Change the Catalog Item Custom Image

- Select the Catalog Item to upload a custom image to
- Click on Browse and select Image to use

**Custom Image**

No custom image has been uploaded.

No file selected. \* Requirements - Type: jpg/png Size: 100x100

- Now you will see the custom image for the Catalog Item be updated

Custom Image



Browse...

No file selected.

\* Requirements - Type: jpg/png Size: 100x100

### 3.22.4 Create New Catalog Bundle

- Go to Services > Catalog > Click on "Catalog Items" menu on the left hand side
- Select the Catalog that was previously created
- Click the "Configuration" Button
- Select "Add a New Catalog Bundle"
- Should bring you to the "Basic Info" Tab
  - Enter the Name and Description and Check the "Display in Catalog"

Basic Info

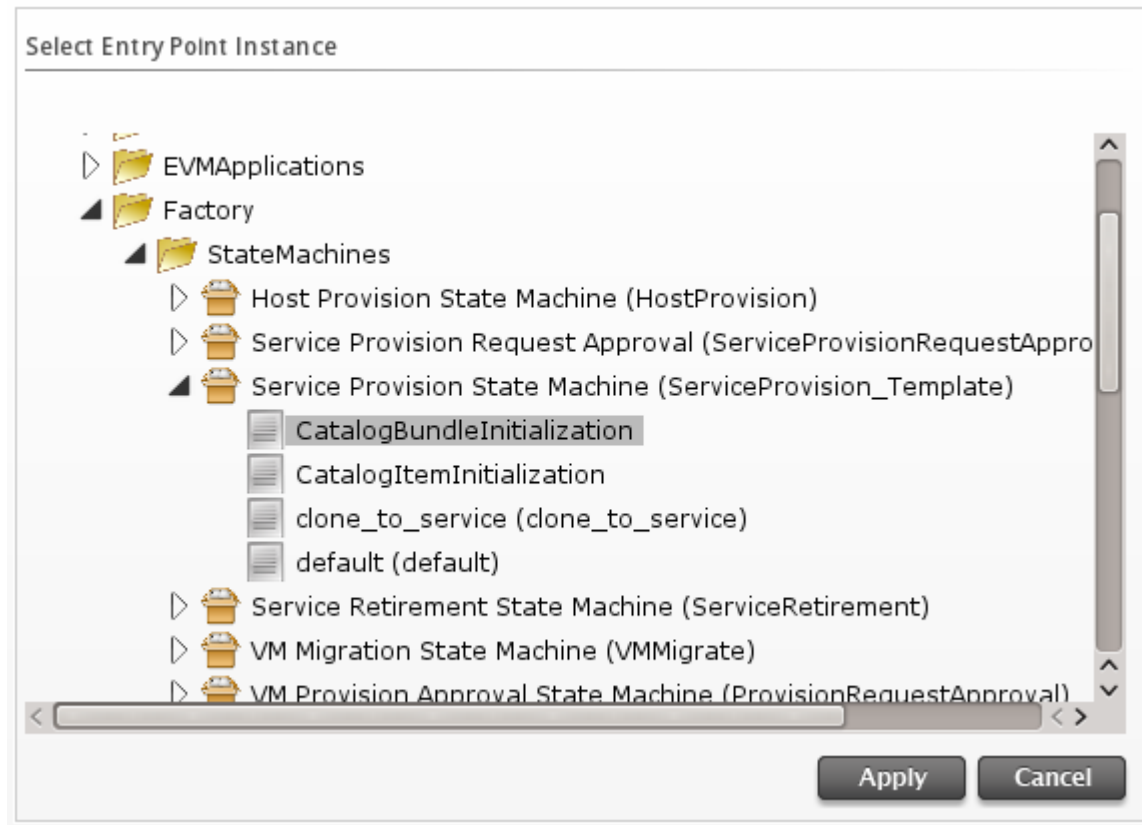
Name / Description	Catalog Bundle Example / Catalog Bundle Example	<input checked="" type="checkbox"/> Display in Catalog
Catalog	001-Dev	
Dialog	blank	
Provisioning Entry Point (NS/CIs/Inst)		
Retirement Entry Point (NS/CIs/Inst)		

- Once the rest of the view is expanded Select the Catalog. i.e. 001-Dev
- Select the Dialog <Blank>

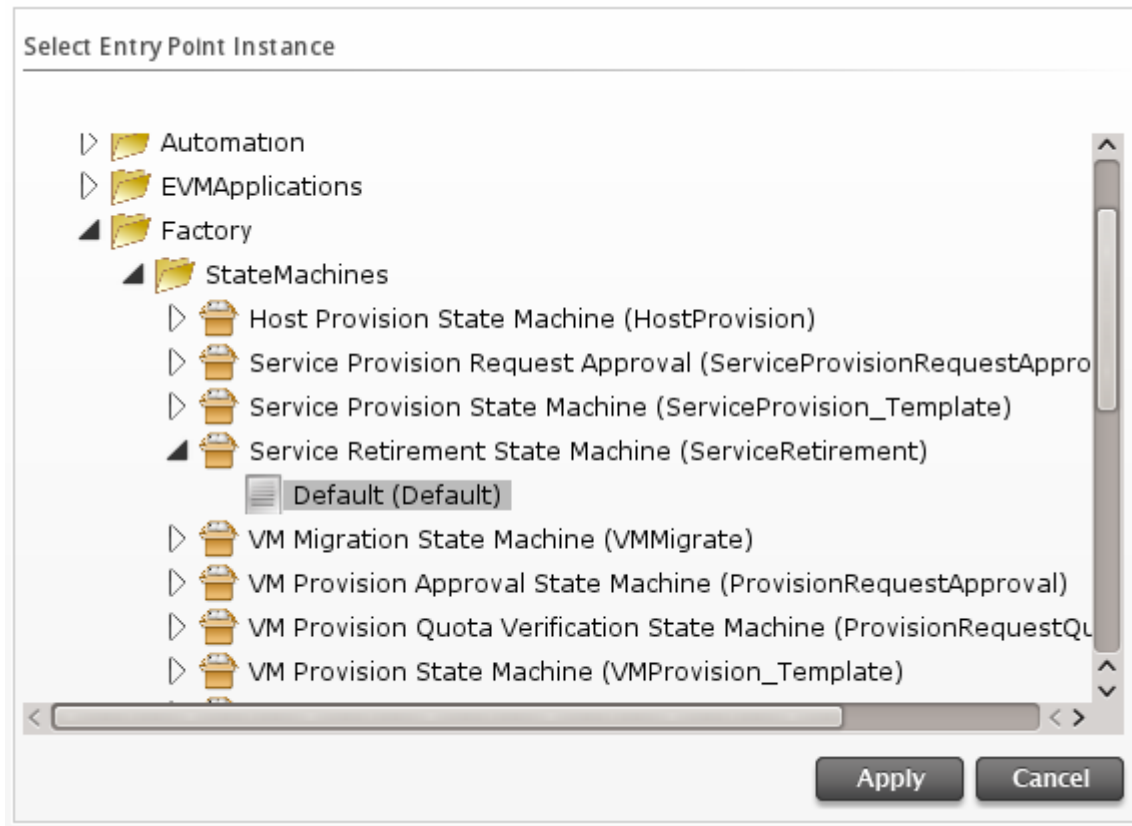
**Important**

You can select another Dialog, but you have to make sure it is for a Bundle and not a single Item)

- Provisioning Entry Point (NS/CIs/Inst): /Factory/StateMachines/ServiceProvision\_Template/CatalogBundleInitialization



- Click Apply
- Retirement Entry Point (NS/CIs/Inst): /Factory/StateMachines/ServiceRetirement/Default



- Click Apply

Basic Info			
Name / Description	Catalog Bundle Example / Catalog Bundle Example	<input checked="" type="checkbox"/> Display in Catalog	
Catalog	001-Dev		
Dialog	blank		
Provisioning Entry Point (NS/CIs/Inst)	Factory/StateMachines/ServiceProvision_Template/Ca		X
Retirement Entry Point (NS/CIs/Inst)	Factory/StateMachines/ServiceRetirement/Default		X

- Click on the "Resources" Tab



- Select an existing Catalog Item Resource (i.e. RHEL 6.4 - Small)
- Select an additional Catalog Item Resource (i.e. RHEL 6.4 - Medium)
- Repeat the previous 2 steps as many times as needed for all of the resources required for this bundle
- If needed, modify the Action Order or Provision Order:

#### Note

Provision Order will only worry about in which order it will actually provision the instance/vm. The Action Order is done once the provisioning is completed it will then perform the action specified in that order. Example: You can have the same Provision Order, but only care about the order that things are powered on.

Selected Resources							
	Name	Action Order	Provision Order	Action		Delay (mins)	
				Start	Stop	Start	Stop
	RHEL 6.4 - Small	1	1	Power On	Shutdown	None	None
	RHEL 6.4 - Medium	2	1	Power On	Shutdown	None	None

- In the above screenshot, "RHEL 6.4 - Small" will power on before "RHEL 6.4 - Medium"
  - Click Add

## 3.23 Cloudforms: Appendix

### 3.23.1 Datastore Import File: [infoblox\\_integration.xml](#)

```
<?xml version="1.0" encoding="UTF-8"?>
<MiqAeDatastore version="1.0">
  <MiqAeClass name="Infoblox_DNS_Entry" namespace="PremierHealthcare/Integration">
    <MiqAeMethod name="Infoblox_DNS_Alias" language="ruby" scope="instance" location="inline"> ←
      <![CDATA[#####
#
# EVM Automate Method: Infoblox_DNS_Alias
#
# Notes: EVM Automate method to add Host entry to Infoblox
#
#####
begin
  @method = 'Infoblox_DNS_Alias'
```

```

$evm.log("info", "==== EVM Automate Method: <#{@method}> Started")

# Turn of verbose logging
@debug = true

require 'rest_client'
require 'json'
require 'nokogiri'
require 'ipaddr'

#####
# Dump Root Vars                                     #
#####
def dump_root()
  $evm.log("info", "Root:<$evm.root> Begin $evm.root.attributes")
  $evm.root.attributes.sort.each { |k, v| $evm.log("info", "Root:<$evm.root> Attribute - #{k} ←
    ): #{v}")}
  $evm.log("info", "Root:<$evm.root> End $evm.root.attributes")
  $evm.log("info", "")
end

#####
# Add DNS Alias                                     #
#####
def addAlias(cname, canonical)
  begin
    url = 'https://' + @connection + '/wapi/v1.0/record:cname'
    content = "{ \"name\": \"#{cname}\", \"canonical\": \"#{canonical}\" }"
    dooie = RestClient.post url, content, :content_type => :json, :accept => :json
    $evm.log("info", "==== EVM Automate Method: <#{@method}> Add Alias inspect: #{dooie. ←
      inspect}")
    return true
  rescue Exception => e
    puts e.inspect
    return false
  end
end

#####
# Testing                                           #
#####

# dump all root attributes to the log
dump_root

vm = $evm.root['vm']

username = nil
username ||= $evm.object['username']

password = nil
password ||= $evm.object.decrypt('password')

servername = nil
servername ||= $evm.object['servername']

dnsdomain = nil
dnsdomain ||= $evm.object['domain']

```

```

dialog_cname = $evm.root.attributes['dialog_cname'] || nil

@name = "#{vm['name']}.#{dnsdomain}"

@connection = "#{username}:#{password}@#{servername}"

uooie = addAlias("#{dialog_cname}.#{dnsdomain}", "#{@name}")
if uooie == true
  $evm.log("info", "==== EVM Automate Method: <#{@method}> Success: #{dialog_cname}.#{ ←
    dnsdomain} to forward to #{@name}")
else
  $evm.log("info", "==== EVM Automate Method: <#{@method}> FAIL: to add DNS Alias of #{ ←
    dialog_cname}.#{dnsdomain} to forward to #{@name}")
  exit MIQ_ABORT
end

#
# Exit method
#
$evm.log("info", "==== EVM Automate Method: <#{@method}> Ended")
exit MIQ_OK

#
# Set Ruby rescue behavior
#
rescue => err
  $evm.log("error", "<#{@method}>: [#{err}]\n#{err.backtrace.join("\n")}")
  exit MIQ_ABORT
end]]> </MiqAeMethod>
  <MiqAeMethod name="Infoblox_Delete_Record" language="ruby" scope="instance" location=" ←
    inline"><![CDATA[#####
#
# EVM Automate Method: Infoblox_Delete_Record
#
# Notes: EVM Automate method to add Host entry to Infoblox
#
#####
begin
  @method = 'Infoblox_Delete_Record'
  $evm.log("info", "==== EVM Automate Method: <#{@method}> Started")

  # Turn of verbose logging
  @debug = true

  require 'rest_client'
  require 'json'
  require 'nokogiri'
  require 'ipaddr'

  #####
  # Dump Root Vars #
  #####
  def dump_root()
    $evm.log("info", "Root:<$evm.root> Begin $evm.root.attributes")
    $evm.root.attributes.sort.each { |k, v| $evm.log("info", "Root:<$evm.root> Attribute - #{k ←
      } : #{v}") }
    $evm.log("info", "Root:<$evm.root> End $evm.root.attributes")
    $evm.log("info", "")
  end
end

```

```
#####
# Fetch Host                                     #
#####
def fetchHost(host)
  begin
    url = 'https://' + @connection + '/wapi/v1.0/record:host?' + "name=#{host}"
    $evm.log("info", "===== #{url.inspect}")
    dooie = RestClient.get url
    $evm.log("info", "===== #{dooie.inspect}")
    doc = Nokogiri::XML(dooie)
    root = doc.root
    hosts = root.xpath("value/_ref/text()")
    hosts.each do | a |
      a = a.to_s
      unless a.index(host).nil?
        puts "Host Found - #{a}"
        return a
      end
    end
    return true
  rescue Exception => e
    puts e.inspect
    return false
  end
end

#####
# Delete Host                                     #
#####
def deleteHost(item)
  begin
    url = 'https://' + @connection + '/wapi/v1.0/' + item
    dooie = RestClient.delete url
    return true
  rescue Exception => e
    puts e.inspect
    return false
  end
end

#####
# Delete Alias                                     #
#####
def deleteAlias(item)
  begin
    url = 'https://' + @connection + '/wapi/v1.0/' + item
    dooie = RestClient.delete url
    $evm.log("info", "==== EVM Automate Method: <#{@method}> Deleting Alias for host - #{ ↔
      @name} Alias: #{item}")
    return true
  rescue Exception => e
    puts e.inspect
    return false
  end
end

#####
# DeleteAliases                                     #
```

```
#####
def findAlias(host)
  begin
    url = 'https://' + @connection + '/wapi/v1.0/record:cname?' + "canonical=#{host}"
    dooie = RestClient.get url
    doc = Nokogiri::XML(dooie)
    root = doc.root
    hosts = root.xpath("value/_ref/text()")
    hosts.each do | a |
      a = a.to_s
      $evm.log("info", "==== EVM Automate Method: <#{@method}> Found Aliases for host - #{ ←
        @name} Alias: #{a}")
      deleteAlias(a)
    end
    return true
  rescue Exception => e
    puts e.inspect
    return false
  end
end

#####
# Testing #
#####

# dump all root attributes to the log
dump_root

vm = $evm.root['vm']

username = nil
username ||= $evm.object['username']

password = nil
password ||= $evm.object.decrypt('password')

servername = nil
servername ||= $evm.object['servername']

dnsdomain = nil
dnsdomain ||= $evm.object['domain']

@name = "#{vm['name']}.#{dnsdomain}"

@connection = "#{username}:#{password}@#{servername}"

$evm.log("info", "==== EVM Automate Method: <#{@method}> Fetching Host: #{@name}")
sooie = fetchHost("#{@name}.#{dnsdomain}")
if sooie == true
  $evm.log("info", "==== EVM Automate Method: <#{@method}> Host: #{@name} does NOT exist")
else
  $evm.log("info", "==== EVM Automate Method: <#{@method}> Fetching Aliases for host - #{ ←
    @name}")
  findAlias(@name)

  $evm.log("info", "==== EVM Automate Method: <#{@method}> Deleting Host - #{sooie}")
  deleteHost(sooie)
end
```

```

#
# Exit method
#
$evm.log("info", "==== EVM Automate Method: <#{@method}> Ended")
exit MIQ_OK

#
# Set Ruby rescue behavior
#
rescue => err
  $evm.log("error", "<#{@method}>: [{err}]\n#{err.backtrace.join("\n")}")
  exit MIQ_ABORT
end]]>      </MiqAeMethod>
  <MiqAeMethod name="Infoblox_Dialog_List_Networks" language="ruby" scope="instance" ↵
    location="inline"><![CDATA[#####]]]
#
# CFME Automate Method: Infoblox_Dialog_List_Networks
#
# Author: Kevin Morey
#
# Notes: This method is executed from a Dynamic Drop-down Service Dialog that will list all ↵
  Infoblox networks and display them in the service dialog
# - gem requirements 'rest_client', 'xmllsimple', 'json'
# dialog_network_cidr
#
#####
begin
  # Method for logging
  def log(level, message)
    @method = 'Infoblox_Dialog_List_Networks'
    $evm.log(level, "#{@method} - #{message}")
  end

  # dump_root
  def dump_root()
    log(:info, "Root:<$evm.root> Begin $evm.root.attributes")
    $evm.root.attributes.sort.each { |k, v| log(:info, "Root:<$evm.root> Attribute - #{k}: #{v ↵
      }") }
    log(:info, "Root:<$evm.root> End $evm.root.attributes")
    log(:info, "")
  end

  # call_infoblox
  def call_infoblox(action, ref='network' )
    require 'rest_client'
    require 'xmllsimple'
    require 'json'

    servername = nil || $evm.object['servername']
    username = nil || $evm.object['username']
    password = nil || $evm.object.decrypt('password')
    url = "https://#{servername}/wapi/v1.0/"+"#{ref}"

    params = {
      :method=>action,
      :url=>url,
      :user=>username,
      :password=>password,

```

```

      :headers=>{ :content_type=>:xml, :accept=>:xml }
    }
    log(:info, "Calling -> Infoblox:<#{url}> action:<#{action}> payload:<#{params[:payload] <-
      ]}>")

    response = RestClient::Request.new(params).execute
    raise "Failure <- Infoblox Response:<#{response.code}>" unless response.code == 200 || <-
      response.code == 201

    log(:info, "Success <- Infoblox Response:<#{response.code}>")
    # use XmlSimple to convert xml to ruby hash
    response_hash = XmlSimple.xml_in(response)
    log(:info, "Inspecting response_hash: #{response_hash.inspect}")
    return response_hash
  end

  # build_dialog
  def build_dialog(hash)
    dialog_field = $evm.object

    # set the values to the dialog_hash
    dialog_field['values'] = hash.keys
    # sort_by: value / description / none
    $evm.object["sort_by"] = "description"
    # sort_order: ascending / descending
    $evm.object["sort_order"] = "ascending"
    # data_type: string / integer
    $evm.object["data_type"] = "string"
    # required: true / false
    $evm.object["required"] = "true"

    log(:info, "Dynamic drop down values: #{ $evm.object['values'] }")
    return $evm.object['values']
  end

  log(:info, "CFME Automate Method Started")

  # dump all root attributes to the log
  dump_root

  # call infoblox to get a list of networks
  networks = call_infoblox(:get)

  # # only pull out the network and the _ref values
  networks_hash = Hash[*networks['value'].collect { |x| [x['network'], x['_ref'][0]] }.flatten <-
    ]
  raise "networks_hash returned nil" if networks_hash.nil?
  log(:info, "Inspecting networks_hash:<#{networks_hash}>")

  build_dialog(networks_hash)

  # Exit method
  log(:info, "CFME Automate Method Ended")
  exit MIQ_OK

  # Set Ruby rescue behavior
rescue => err
  log(:error, "[#{err}]\n#{err.backtrace.join("\n")}")
  exit MIQ_STOP

```

```

end]]>      </MiqAeMethod>
      <MiqAeMethod name="Infoblox_Host_Record" language="ruby" scope="instance" location="inline ←
        "><![CDATA[#####
#
# EVM Automate Method: Infoblox_Host_Record
#
# Notes: EVM Automate method to add Host entry to Infoblox
#
#####
begin
  @method = 'Infoblox_Host_Record'
  $evm.log("info", "==== EVM Automate Method: <#{@method}> Started")

  # Turn of verbose logging
  @debug = true

  require 'rest_client'
  require 'json'
  require 'nokogiri'
  require 'ipaddr'

  #####
  # Dump Root Vars          #
  #####
  def dump_root()
    $evm.log("info", "Root:<$evm.root> Begin $evm.root.attributes")
    $evm.root.attributes.sort.each { |k, v| $evm.log("info", "Root:<$evm.root> Attribute - #{k ←
      } : #{v}")}
    $evm.log("info", "Root:<$evm.root> End $evm.root.attributes")
    $evm.log("info", "")
  end

  #####
  # Fetch Host              #
  #####
  def fetchHost(host)
    begin
      url = 'https://' + @connection + '/wapi/v1.0/record:host?' + "name=#{host}"
      $evm.log("info", "===== #{url.inspect}")
      dooie = RestClient.get url
      $evm.log("info", "===== #{dooie.inspect}")
      doc = Nokogiri::XML(dooie)
      root = doc.root
      hosts = root.xpath("value/_ref/text()")
      hosts.each do | a |
        a = a.to_s
        unless a.index(host).nil?
          puts "Host Found - #{a}"
          return a
        end
      end
      return true
    rescue Exception => e
      puts e.inspect
      return false
    end
  end

  #####

```



```

# Delete Host
#####
def deleteHost(item)
  begin
    url = 'https://' + @connection + '/wapi/v1.0/' + item
    dooie = RestClient.delete url
    return true
  rescue Exception => e
    puts e.inspect
    return false
  end
end

#####
# Get IP Address
#####
def getIP(hostname, ipaddress)
  begin
    url = 'https://' + @connection + '/wapi/v1.0/record:host'
    content = "\\{ \"ipv4addrs\":\\[\\{ \"ipv4addr\":\\\"#{ipaddress}\\\"\\}\\],\\\"name\":\\\"#{hostname} ←
    }\\\"}"
    dooie = RestClient.post url, content, :content_type => :json, :accept => :json
    return true
  rescue Exception => e
    puts e.inspect
    return false
  end
end

#####
# Fetch Network Ref
#####
def fetchNetworkRef(cdir)
  begin
    $evm.log("info", "GetIP --> Network Search - #{cdir}")
    url = 'https://' + @connection + '/wapi/v1.0/network'
    dooie = RestClient.get url
    doc = Nokogiri::XML(dooie)
    root = doc.root
    networks = root.xpath("value/_ref/text()")
    networks.each do | a |
      a = a.to_s
      unless a.index(cdir).nil?
        $evm.log("info", "==== EVM Automate Method: <#{@method}> GetIP --> Network Found - ←
        #{a}")
        return a
      end
    end
    return nil
  rescue Exception => e
    $evm.log("info", "==== EVM Automate Method: <#{@method}> #{e.inspect}")
    return false
  end
end

#####
# Next Available IP Address
#####
def nextIP(network)

```

```

begin
  $evm.log("info","NextIP on - #{network}")
  url = 'https://' + @connection + '/wapi/v1.0/' + network
  dooie = RestClient.post url, :_function => 'next_available_ip', :num => '1'
  doc = Nokogiri::XML(dooie)
  root = doc.root
  nextip = root.xpath("ips/list/value/text()")
  $evm.log("info", "==== EVM Automate Method: <#{@method}> NextIP is - #{nextip}")
  return nextip
rescue Exception => e
  $evm.log("info", "==== EVM Automate Method: <#{@method}> #{e.inspect}")
  return false
end
end

#####
#
# Method: validate_ipaddr
# Notes: This method uses a regular expression to validate the ipaddr and gateway
# Returns: Returns string: true/false
#
#####
def validate_ipaddr(ip)
  ip_regex = /\b(?:?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\b/
  if ip_regex =~ ip
    $evm.log("info","IP Address:<#{ip}> passed validation") if @debug
    return true
  else
    $evm.log("error","IP Address:<#{ip}> failed validation") if @debug
    return false
  end
end

#####
# Set Options in prov #
#####
def set_prov(prov, hostname, ipaddr, netmask, gateway)
  $evm.log("info", "GetIP --> Hostname = #{hostname}")
  $evm.log("info", "GetIP --> IP Address = #{ipaddr}")
  $evm.log("info", "GetIP --> Netmask = #{netmask}")
  $evm.log("info", "GetIP --> Gateway = #{gateway}")
  prov.set_option(:sysprep_spec_override, 'true')
  prov.set_option(:addr_mode, ["static", "Static"])
  prov.set_option(:ip_addr, "#{ipaddr}")
  prov.set_option(:subnet_mask, "#{netmask}")
  prov.set_option(:gateway, "#{gateway}")
  prov.set_option(:vm_target_name, "#{hostname}")
  prov.set_option(:linux_host_name, "#{hostname}")
  prov.set_option(:vm_target_hostname, "#{hostname}")
  prov.set_option(:host_name, "#{hostname}")
  $evm.log("info", "GetIP --> #{prov.inspect}")
  $evm.log("info", "GetIP --> #{prov.get_option(:ip_addr)}")
end

#####
# Set netmask #
#####

```

```

def netmask(cdir)
  netblock = IPAddr.new(cdir)
  netins = netblock.inspect
  netmask = netins.match(/(?<=\/) (.*) (?=>\/)/)
  $evm.log("info", "GetIP --> Netmask = #{netmask}")
  return netmask
end

#####
# Testing                                     #
#####

# dump all root attributes to the log
dump_root

action = nil
action ||= $evm.object['action'] || $evm.root['action']
$evm.log("info", "GetIP --> Action= #{action}")

username = nil
username ||= $evm.object['username']

password = nil
password ||= $evm.object.decrypt('password')

servername = nil
servername ||= $evm.object['servername']

subnet = nil
subnet ||= $evm.object['subnet']

gateway = nil
gateway ||= $evm.object['gateway']

dnsdomain = nil
dnsdomain ||= $evm.object['domain']

# Get vm from miq_provision object
prov = $evm.root["miq_provision"]
$evm.log("info", "#{prov.inspect}")

vm_name = prov.options[:vm_target_name]
$evm.log("info", "GetIP --> VM Name = #{vm_name}")

vm_dest_id = prov['destination_id'].to_i
$evm.log("info", "GetIP --> vm_dest_id = #{vm_dest_id.inspect}")

vm_data = $evm.vmdb('vm', vm_dest_id) unless vm_dest_id == 0
$evm.log("info", "GetIP --> vm_data = #{vm_data.inspect}")

ipaddress = vm_data.ipaddresses[0]
$evm.log("info", "GetIP --> IP Address = #{ipaddress}")

@name = "#{vm_name}.#{dnsdomain}"
raise "VM Name was not passed" if @name.empty?

@connection = "#{username}:#{password}@#{servername}"

```

```

if vm_data['vendor'] == 'openstack'
  $evm.log("info", "==== EVM Automate Method: <#{@method}> Vendor Type: #{vm_data['vendor'] ←
    '}} Running Infoblox Integration")
  case action

    when "verifyhost"
      $evm.log("info", "==== EVM Automate Method: <#{@method}> Verifying Host: #{@name}.#{ ←
        dnsdomain}")
      sooie = fetchHost("#{@name}.#{dnsdomain}")
      if sooie == true
        $evm.log("info", "==== EVM Automate Method: <#{@method}> Host: #{@name}.#{dnsdomain ←
          } does NOT exist")
      else
        $evm.log("info", "==== EVM Automate Method: <#{@method}> Host: #{@name}.#{dnsdomain ←
          } does exist")
      end

    when "createhost"
      ipadd = '10.32.18.55'
      $evm.log("info", "==== EVM Automate Method: <#{@method}> IPADD: #{ipadd.inspect} #{ ←
        ipadd.class} -> IPADDRESS #{ipaddress.inspect} #{ipaddress.class}")
      uooie = getIP("#{@name}.#{dnsdomain}", "#{ipaddress}")
      if uooie == true
        $evm.log("info", "==== EVM Automate Method: <#{@method}> #{@name}.#{dnsdomain} with ←
          IP Address #{ipaddress} created successfully")
      elsif uooie == false
        $evm.log("info", "==== EVM Automate Method: <#{@method}> #{@name}.#{dnsdomain} with ←
          IP Address #{ipaddress} FAILED")
        exit MIQ_ABORT
      else
        $evm.log("info", "==== EVM Automate Method: <#{@method}> unknown error")
        exit MIQ_ABORT
      end

    when "getipnext"
      netRef = fetchNetworkRef(subnet)
      nextIPADDR = nextIP(netRef)
      $evm.log("info", "==== EVM Automate Method: <#{@method}> GetIPNext-before --> #{prov. ←
        options[:vm_target_name]}.#{dnsdomain} with IP Address #{nextIPADDR} created ←
        successfully")
      result = getIP("#{prov.options[:vm_target_name]}.#{dnsdomain}", nextIPADDR)
      $evm.log("info", "==== EVM Automate Method: <#{@method}> GetIPNext-after --> #{prov. ←
        options[:vm_target_name]}.#{dnsdomain} with IP Address #{nextIPADDR} created ←
        successfully")
      if result == true
        $evm.log("info", "==== EVM Automate Method: <#{@method}> GetIP --> #{prov.options[ ←
          :vm_target_name]}.#{dnsdomain} with IP Address #{nextIPADDR} created ←
          successfully")
        netmask = netmask(subnet)
        set_prov(prov, prov.options[:vm_target_name], nextIPADDR, netmask, gateway)
      elsif result == false
        $evm.log("info", "==== EVM Automate Method: <#{@method}> GetIP --> #{prov.options[ ←
          :vm_target_name]}.#{dnsdomain} with IP Address #{nextIPADDR} FAILED")
        exit MIQ_ABORT
      else
        $evm.log("info", "==== EVM Automate Method: <#{@method}> GetIP --> unknown error")
      end

  end

end

```

```

else
  $evm.log("info", "==== EVM Automate Method: <#{@method}> Vendor Type: #{vm_data['vendor']}} skipping Infoblox Integration")
end

#
# Exit method
#
$evm.log("info", "==== EVM Automate Method: <#{@method}> Ended")
exit MIQ_OK

#
# Set Ruby rescue behavior
#
rescue => err
  $evm.log("error", "<#{@method}>: [#{err}]\n#{err.backtrace.join("\n")}")
  exit MIQ_ABORT
end]]> </MiqAeMethod>
  <MiqAeSchema>
    <MiqAeField name="servername" substitute="true" aetype="attribute" datatype="string"
      priority="1" message="create">
10.32.2.200 </MiqAeField>
    <MiqAeField name="username" substitute="true" aetype="attribute" datatype="string"
      priority="2" message="create">
cloudforms </MiqAeField>
    <MiqAeField name="password" substitute="true" aetype="attribute" datatype="password"
      priority="3" message="create">
v1:{ax0hEkT5S7cKfKI5JEo3uw==} </MiqAeField>
    <MiqAeField name="to_email_address" substitute="true" aetype="attribute" datatype="
      string" priority="4" message="create">
    </MiqAeField>
    <MiqAeField name="from_email_address" substitute="true" aetype="attribute" datatype="
      string" priority="5" message="create">
    </MiqAeField>
    <MiqAeField name="signature" substitute="true" aetype="attribute" datatype="string"
      priority="6" message="create">
    </MiqAeField>
    <MiqAeField name="action" substitute="true" aetype="attribute" datatype="string"
      priority="7" message="create">
    </MiqAeField>
    <MiqAeField name="gateway" substitute="true" aetype="attribute" datatype="string"
      priority="8" message="create">
10.32.18.1 </MiqAeField>
    <MiqAeField name="subnet" substitute="true" aetype="attribute" datatype="string"
      priority="9" message="create">
10.32.18.0/23 </MiqAeField>
    <MiqAeField name="domain" substitute="true" aetype="attribute" datatype="string"
      priority="10" message="create">
premierinc.com </MiqAeField>
    <MiqAeField name="method1" substitute="true" aetype="method" datatype="string" priority=
      "11" message="create">
    </MiqAeField>
    <MiqAeField name="method2" substitute="true" aetype="method" datatype="string" priority=
      "12" message="create">
    </MiqAeField>
  </MiqAeSchema>
  <MiqAeInstance name="Infoblox_DNS_Alias">
    <MiqAeField name="servername">

```

```

        <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="username">
        <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="password">
        <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="to_email_address">
        <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="from_email_address">
        <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="signature">
        <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="action">
        <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="gateway">
        <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="subnet">
        <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="domain">
        <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="method1">
Infoblox_DNS_Alias    </MiqAeField>
    <MiqAeField name="method2">
        <![CDATA[]]>
    </MiqAeField>
</MiqAeInstance>
<MiqAeInstance name="Infoblox_Dialog_List_Networks">
    <MiqAeField name="servername">
        <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="username">
        <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="password">
        <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="to_email_address">
        <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="from_email_address">
        <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="signature">
        <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="action">
        <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="gateway">
        <![CDATA[]]>

```

```

    </MiqAeField>
    <MiqAeField name="subnet">
      <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="domain">
      <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="method1">
Infoblox_Dialog_List_Networks    </MiqAeField>
    <MiqAeField name="method2">
      <![CDATA[]]>
    </MiqAeField>
  </MiqAeInstance>
  <MiqAeInstance name="Infoblox_Host_Record">
    <MiqAeField name="servername">
      <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="username">
      <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="password">
      <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="to_email_address">
      <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="from_email_address">
      <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="signature">
      <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="action">
      <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="method1">
Infoblox_Host_Record    </MiqAeField>
    <MiqAeField name="method2">
      <![CDATA[]]>
    </MiqAeField>
  </MiqAeInstance>
  <MiqAeInstance name="Infoblox_Instance_Provision">
    <MiqAeField name="servername">
      <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="username">
      <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="password">
      <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="to_email_address">
      <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="from_email_address">
      <![CDATA[]]>
    </MiqAeField>
    <MiqAeField name="signature">
      <![CDATA[]]>

```

```

        </MiqAeField>
        <MiqAeField name="action">
createhost      </MiqAeField>
        <MiqAeField name="gateway">
            <![CDATA[]]>
        </MiqAeField>
        <MiqAeField name="subnet">
            <![CDATA[]]>
        </MiqAeField>
        <MiqAeField name="domain">
            <![CDATA[]]>
        </MiqAeField>
        <MiqAeField name="method1">
Infoblox_Host_Record    </MiqAeField>
        <MiqAeField name="method2">
            <![CDATA[]]>
        </MiqAeField>
    </MiqAeInstance>
    <MiqAeInstance name="Infoblox_Instance_Retire">
        <MiqAeField name="servername">
            <![CDATA[]]>
        </MiqAeField>
        <MiqAeField name="username">
            <![CDATA[]]>
        </MiqAeField>
        <MiqAeField name="password">
            <![CDATA[]]>
        </MiqAeField>
        <MiqAeField name="to_email_address">
            <![CDATA[]]>
        </MiqAeField>
        <MiqAeField name="from_email_address">
            <![CDATA[]]>
        </MiqAeField>
        <MiqAeField name="signature">
            <![CDATA[]]>
        </MiqAeField>
        <MiqAeField name="action">
            <![CDATA[]]>
        </MiqAeField>
        <MiqAeField name="gateway">
            <![CDATA[]]>
        </MiqAeField>
        <MiqAeField name="subnet">
            <![CDATA[]]>
        </MiqAeField>
        <MiqAeField name="domain">
            <![CDATA[]]>
        </MiqAeField>
        <MiqAeField name="method1">
Infoblox_Delete_Record    </MiqAeField>
        <MiqAeField name="method2">
            <![CDATA[]]>
        </MiqAeField>
    </MiqAeInstance>
    <MiqAeInstance name="Infoblox_Instance_Verify">
        <MiqAeField name="servername">
            <![CDATA[]]>
        </MiqAeField>

```



```
<MiqAeField name="username">
  <![CDATA[]]>
</MiqAeField>
<MiqAeField name="password">
  <![CDATA[]]>
</MiqAeField>
<MiqAeField name="to_email_address">
  <![CDATA[]]>
</MiqAeField>
<MiqAeField name="from_email_address">
  <![CDATA[]]>
</MiqAeField>
<MiqAeField name="signature">
  <![CDATA[]]>
</MiqAeField>
<MiqAeField name="action">
verifyhost      </MiqAeField>
  <MiqAeField name="method1">
Infoblox_Host_Record      </MiqAeField>
  <MiqAeField name="method2">
    <![CDATA[]]>
  </MiqAeField>
</MiqAeInstance>
</MiqAeClass>
</MiqAeDatastore>
```

## 4 Issues Encountered