Vbrick Best Practices Guide

v1.0.0 – August 2018

607 Herndon Parkway, Suite 300 \ Herndon, VA 20171 \ USA \ www.vbrick.com

Table of Contents

Introduction

Overview

This guide summarizes the best practices that Vbrick teams follow while installing, configuring and maintaining Rev in the cloud or on-premises. This guide does not provide the installation steps. Please view the implementation documents that are available online and in the Vbrick website customer/partner portal. Please refer to the Appendix of this document for more links to these documents.

Rev Installation (On-premises)

Overview

This guide does not give the installation steps for Rev. It summarizes the best practices that V Vbrick Brick teams follow while installing Rev. For more details on installation, please refer to VBU content through ICP certification. Also, please view the implementation documents that are available online and in the Vbrick website as well the installation documents that can be requested from Vbrick support team. Please refer to the Appendix of this document for more links to these documents.

Architecture and Design

The Rev video management and webcasting platform depends upon the size of the system needed by the customer. The system should be sized using the Server and VM Sizing and Capacities found in section 1.2.2. The supported system configurations are Multi-Node and Single-Node.

The Rev platform consists of four primary components:

- Rev Runtime server
- MongoDB Server
- ElasticSearch Server
- Video Storage

RUNTIME

The Rev run-time layer is the “brains” behind the Rev application and provides a variety of functions:

- Web application
- Security and access control
- Media management
- Transcoding
- Logging
- Workflow
- Authorization
- Message Bus & Clustering

In addition to the direct functions, the runtime layer is also the interface to the persistency layers associated with the system including MongoDB, ElasticSearch, and the Video Storage layer. The runtime layer is hosted via Windows 2012 R2 physical or virtual servers, and can be clustered for high availability.

MONGODB

The MongoDB layer is the primary persistency layer within the Rev ecosystem. It contains all metadata associated to the system and its contents including:

- System state
- Local users & authentication information
- Remote (LDAP/SSO) users, metadata only
- Video Metadata
- GUIDs
- Titles
- Descriptions
- Access Control
- Status, feature, thumbnails
- Video organizational information
- Categories
- Keywords
- Tags
- System branding and other functions.

The MongoDB layer is hosted via Linux provided customer system either on a physical or virtual server. As with the runtime layer, the MongoDB layer can be installed in a single node or multi- node installation to allow for high availability.

ELASTIC SEARCH

The Elastic Search layer indexes the data available in the MongoDB layer and provides searching capabilities. This is a persistency layer in that it provides critical services to the Rev run time both for video access, browsing and playback and actual video searching, but unlike the MongoDB, no state information is stored here, and if necessary the Elastic Search information can be rebuilt directly from the MongoDB layer.

The Elastic Search layer is hosted via Linux provided customer system either on a physical or virtual server. As with the runtime layer, the Elastic Search layer can be installed in a single node or multi node installation to allow for high availability.

VIDEO STORAGE

Customers must provide video storage to the Rev run-time in a format that can be mounted as a Windows 2012 Server drive letter or UNC path. The format of this storage can range from simple hardware disks, to Network Attached Storage (NAS), to redundant Storage Area Network (SAN) storage as long as it can be mounted by Windows via SMB. The same network drive should be mounted on all runtime servers and should be redundant and/or regularly backed up. (See the Server and VM Sizing and Capacities found in section 1.2.2 for drive size and performance requirements.).

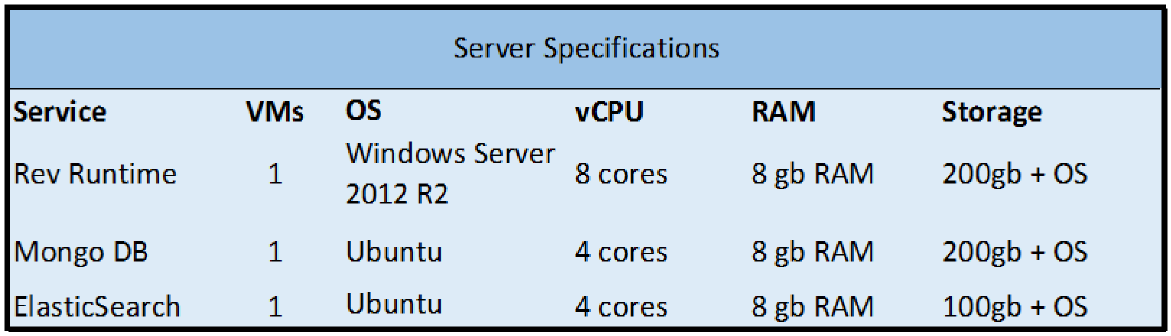
SERVER / VM SIZING AND CAPABILITIES

The Rev platform is elastic in nature and will dynamically scale up and scale down to meet incoming load as needed, however Rev On-Premise is limited to the hardware footprint. So to accurately determine the correct hardware requirements for a Rev On-Premise install the sizing factors should be considered.

For small deployments, the first choice is between a highly available and non-highly available system (see the 1.2.1. Rev Solution Server Architecture section for more information regarding this choice). Other factors include:

- Primary Use Case: Live Webcasts or On-Demand
- Expected Total User Count
- Expected Concurrent User Count
- Hours of VOD Content

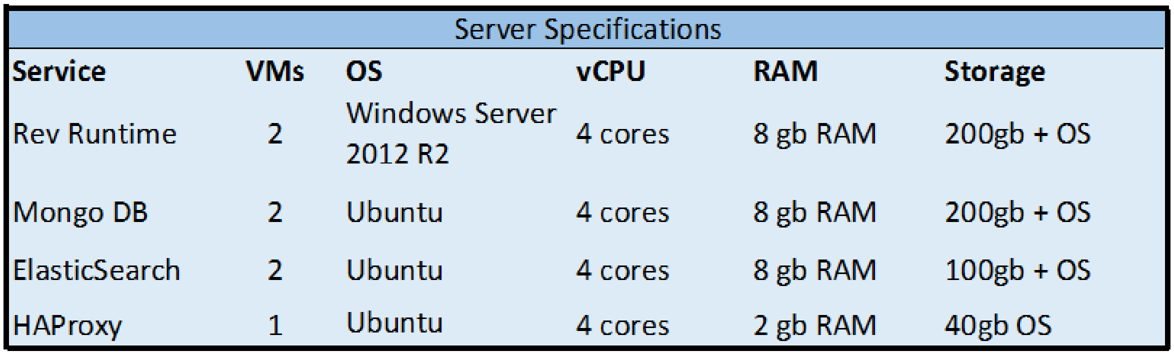
The minimum non-redundant deployment is:



Server Specifications

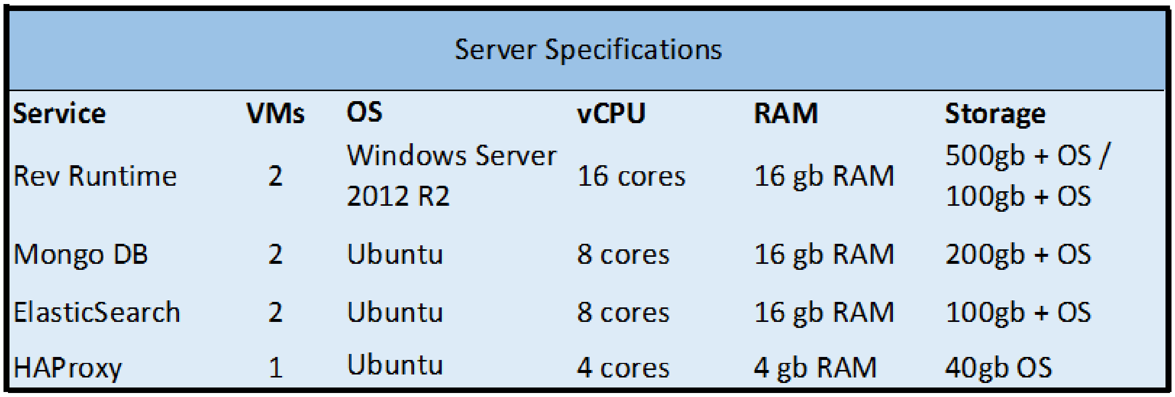
Service	VMs	OS	vCPU	RAM	Storage
Rev Runtime	1	Windows Server 2012 R2	8 cores	8 gb RAM	200gb + OS
Mongo DB	1	Ubuntu	4 cores	8 gb RAM	200gb + OS
ElasticSearch	1	Ubuntu	4 cores	8 gb RAM	100gb + OS

The minimum redundant deployment is:



Server Specifications					
Service	**VMs**	**OS**	**vCPU**	**RAM**	**Storage**
Rev Runtime	2	Windows Server 2012 R2	4 cores	8 gb RAM	200gb + OS
Mongo DB	2	Ubuntu	4 cores	8 gb RAM	200gb + OS
ElasticSearch	2	Ubuntu	4 cores	8 gb RAM	100gb + OS
HAProxy	1	Ubuntu	4 cores	2 gb RAM	40gb OS

The preferred redundant deployment is:



Server Specifications					
Service	**VMs**	**OS**	**vCPU**	**RAM**	**Storage**
Rev Runtime	2	Windows Server 2012 R2	16 cores	16 gb RAM	500gb + OS / 100gb + OS
Mongo DB	2	Ubuntu	8 cores	16 gb RAM	200gb + OS
ElasticSearch	2	Ubuntu	8 cores	16 gb RAM	100gb + OS
HAProxy	1	Ubuntu	4 cores	4 gb RAM	40gb OS

LOAD BALANCER

For on-premise applications that are Multi-Node, customers have a choice of load balancing; Single-Node does not require Load Balancing.

The Vbrick provided software includes the ability to load an HA-Proxy load balancer. The HA-Proxy load balancer is hosted via linux provided customer system either on a physical or virtual server. Customers have the option of using Hardware Load Balancers such as an F5 or a Barracuda Load Balancer but the customer will be responsible for providing the hardware and implementing the Load Balancing solution on the hardware.

For on- premise installs expecting less than 5000 concurrent users, the HA Proxy load balancer will be sufficient, although it does represent a single point of failure.

In either scenario, the load balancer is used to proxy initial connections to the Rev Runtime web service. Work performed within the Rev Runtime and between the Rev Runtime and the persistency layers is automatically load balanced already.

Hardware-based load balancing generally works at the network appliance (router or switch) level. The load balancer will examine the network packets (at one or more layers of the OSI model) and route them accordingly. There are various methods for routing the traffic in a load-balanced manner, including NAT (IP address translation), tunneling, and direct routing.

Since the Rev Servers is a stateless application, the issue of session persistence (or stickiness) is not generally a consideration. Therefore, load balancing the Rev Servers becomes a network exercise based on the capabilities of the network hardware. Similarly, the ability of the hardware to interact with the servers and/or the application will dictate how well the hardware can determine if servers are alive and how they are faring against load fluctuations.

If the customer is implementing an HTTPS solution the certificate for the system must be placed on the HA Proxy server or hardware load balancer as the Load Balancer must be the HTTPS endpoint. OpenSSL commands need to be run to generate the SSL Certificate request and the private key file. Once the certificates are issued they need to be placed on the HA Proxy server or hardware load balancer. After this you will need to tell the Load Balancer about the two Rev servers to balancing the traffic between the nodes. See the “SSL certificate process for HAProxy guide” for detailed instructions on how to configure HTTPS on a HA Proxy server. For Hardware Load Balancers customers will need to consult the manufacturer’s guide on how to implement an SSL Certificate and load balance between the Rev servers.

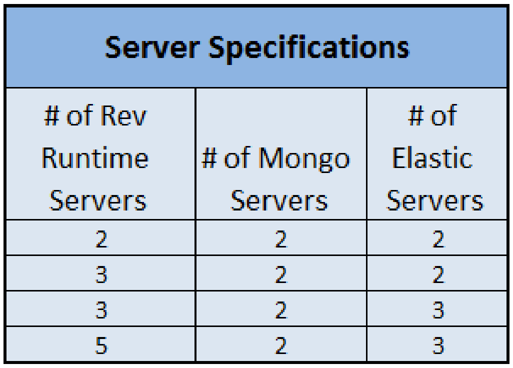
HA PROXY SERVER

The other use of an HA Proxy server is to use the Vbrick Automatic Setup node which saves time and reduces the chance of error. This can be done only for on-premise applications that are Multi-Node or Single-Node using the Vbrick provided software.

This Automatic Setup component allows the installer to load the HA Proxy, Elasticsearch Node(s), MongoDB Node(s), Vbrick Rev Node(s), IP addresses, Hostname, Domain Name, FQDN, Subnet Mask, Gateway, DNS IPaddres(s) (DNS 1 and DNS 2) into the installer program one time. The HA Proxy server will save a file called vbrick-vars.txt on it that will be used for the installation and configuration of the Nodes. See the Rev On-Premise guide for detailed instructions on how to use the Automatic Setup Feature.

Supported Server Configuration

The supported version of the Vbrick Rev system is Single-Node and Multi-Node. As per the Rev Sizing Guide the Multi-Node configuration can be anyone of the following configurations based on Concurrent Users for the Live Use Case and/or based on the VOD Use Case



Server Specifications		
# of Rev Runtime Servers	# of Mongo Servers	# of Elastic Servers
2	2	2
3	2	2
3	2	3
5	2	3

Install the On-Premises System

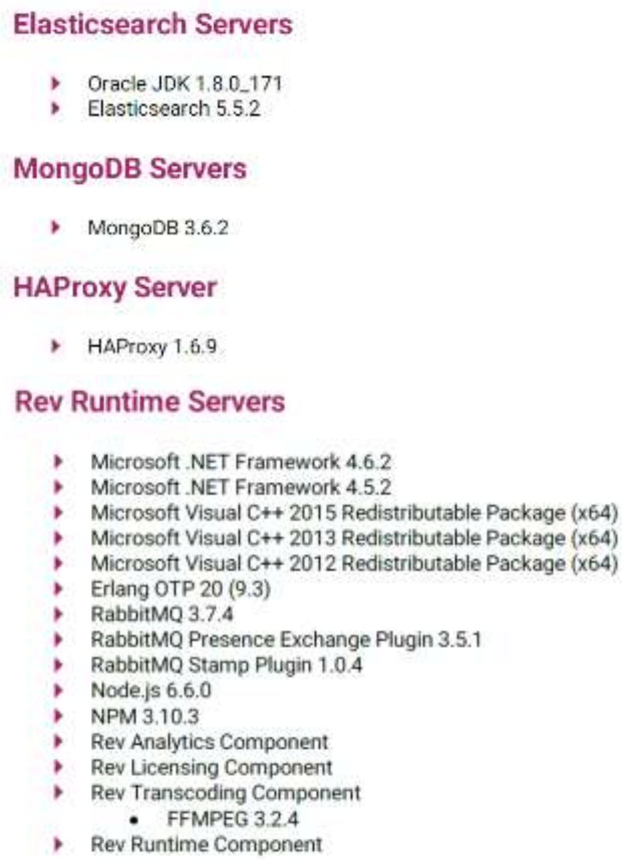
SOFTWARE AND NOTES

Beginning with release 7.22, Vbrick has dropped direct Operating System support. In previous releases, an ISO-based installer could be used to deploy hardware or virtual machines with Ubuntu 14.04 and all the packaging necessary to support the desired role for that device. For 7.22 Vbrick will no longer distribute the ISO image, instead we're releasing a Package Installer that works similar in many ways to previous installers but provides support for both Ubuntu 14.04 and Red Hat Enterprise Server 7. The change in installers allows Enterprise Customers to use their own machine deployments.

These notes are best practices for how to install the system manually, for Installation instructions please refer to the Step-by-Step Installation Guide from Vbrick Engineering.

At a minimum five (5) Linux servers and two (2) Windows servers need to be created for a multinode installation. It is assumed that you are using the HA Proxy Load Balancer feature rather than using a hardware Load Balancer as discussed in section 1.2.3.1. First load your preferred operating system and back up all of the servers. Backing up the servers allows us to revert back to the OS if the system does not install properly. If you do not want to back up the servers then you can always remove the HAProxy, Elastic and Mongo software and re-install as a troubleshooting step.

Depending upon what version of Vbrick Rev software you are trying to install the components that are used are documented in the Vbrick Rev On-Premise Installation Guide. Below is are the software versions from the 7.22 Rev On-Premise file (See the “Server Layout & Software Installed” of the Rev OnPremises Installation Guide).



Elasticsearch Servers

- Oracle JDK 1.8.0_171
- Elasticsearch 5.5.2

MongoDB Servers

- MongoDB 3.6.2

HAProxy Server

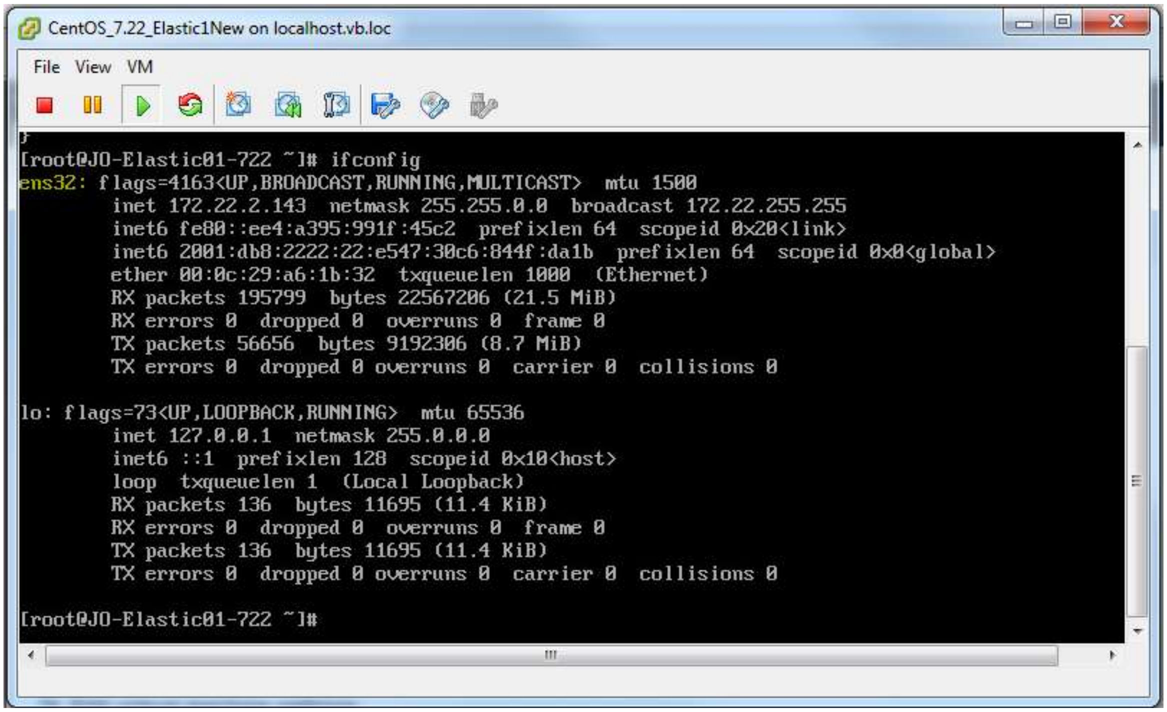
- HAProxy 1.6.9

Rev Runtime Servers

- Microsoft .NET Framework 4.6.2
- Microsoft .NET Framework 4.5.2
- Microsoft Visual C++ 2015 Redistributable Package (x64)
- Microsoft Visual C++ 2013 Redistributable Package (x64)
- Microsoft Visual C++ 2012 Redistributable Package (x64)
- Erlang OTP 20 (9.3)
- RabbitMQ 3.7.4
- RabbitMQ Presence Exchange Plugin 3.5.1
- RabbitMQ Stamp Plugin 1.0.4
- Node.js 6.6.0
- NPM 3.10.3
- Rev Analytics Component
- Rev Licensing Component
- Rev Transcoding Component
    - FFMPEG 3.2.4
- Rev Runtime Component

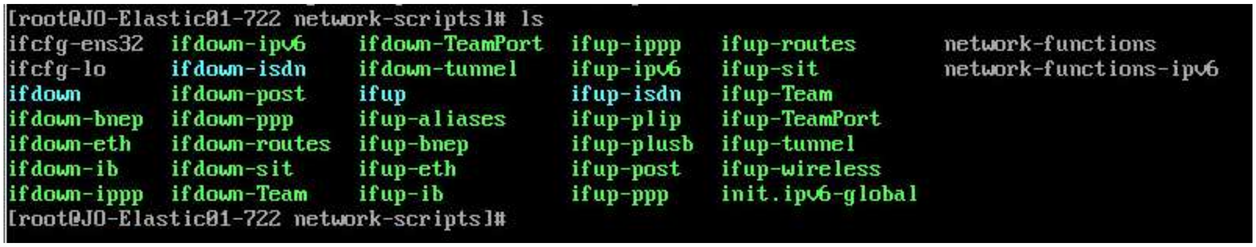
NETWORK ACCESS

The servers will all need network access to copy the vbrick-packageinstall-7.22_XX.tar.gz file. Run an ifconfig to determine the name of the LAN connection.



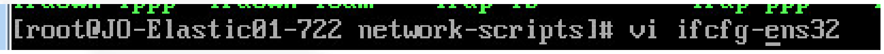
```
}
[root@JO-Elastic01-722 ~]# ifconfig
ens32: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.22.2.143  netmask 255.255.0.0  broadcast 172.22.255.255
        inet6 fe80::ee4:a395:991f:45c2  prefixlen 64  scopeid 0x20<link>
        inet6 2001:db8:2222:22:e547:30c6:844f:da1b  prefixlen 64  scopeid 0x0<global>
        ether 00:0c:29:a6:1b:32  txqueuelen 1000  (Ethernet)
        RX packets 195799  bytes 22567206 (21.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 56656  bytes 9192306 (8.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 136  bytes 11695 (11.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 136  bytes 11695 (11.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@JO-Elastic01-722 ~]#
```

If the file is set up as DHCP then change the LAN file to a static IP address. The file is located in the /etc/sysconfig/network-scripts folder. In this example the LAN connection is exs32 therefore the file that needs to change is the ifcfg-ens32 file.

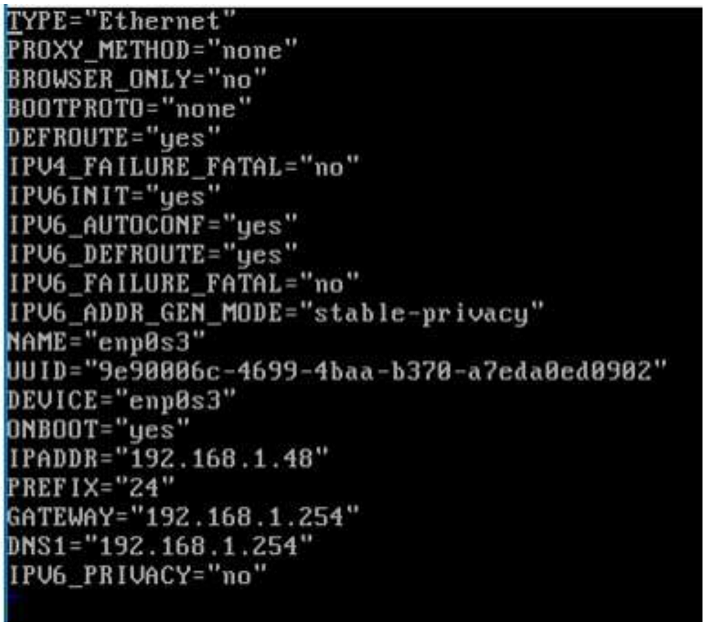


```
[root@JO-Elastic01-722 network-scripts]# ls
ifcfg-ens32  ifdown-ipv6    ifdown-TeamPort  ifup-ippp    ifup-routes       network-functions
ifcfg-lo     ifdown-isdn    ifdown-tunnel    ifup-ipv6    ifup-sit          network-functions-ipv6
ifdown       ifdown-post    ifup             ifup-isdn    ifup-Team
ifdown-bnep  ifdown-ppp     ifup-aliases     ifup-plip    ifup-TeamPort
ifdown-eth   ifdown-routes  ifup-bnep        ifup-plusb   ifup-tunnel
ifdown-ib    ifdown-sit     ifup-eth         ifup-post    ifup-wireless
ifdown-ippp  ifdown-Team    ifup-ib          ifup-ppp     init.ipv6-global
[root@JO-Elastic01-722 network-scripts]#
```

Edit the file to set the static IP addresses for the servers.



```
[root@JO-Elastic01-722 network-scripts]# vi ifcfg-ens32
```



```
TYPE="Ethernet"
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="none"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="enp0s3"
UUID="9e90006c-4699-4baa-b370-a7eda0ed0902"
DEVICE="enp0s3"
ONBOOT="yes"
IPADDR="192.168.1.48"
PREFIX="24"
GATEWAY="192.168.1.254"
DNS1="192.168.1.254"
IPV6_PRIVACY="no"
```

Add in the Static IP addresses. Use :wq to write and quit VI editor.

Restart the Network Interface:

systemctl restart network

Check the status of the Network connection

systemctl status network

Confirm Network access by pinging the default gateway

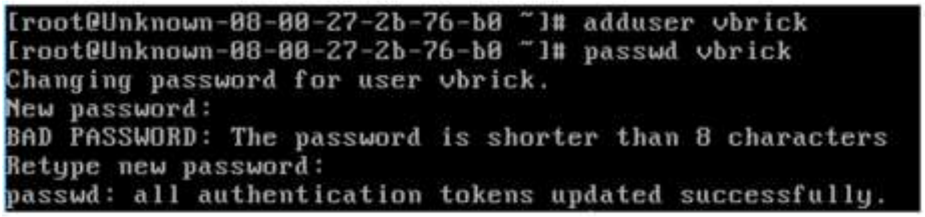
Ping 192.168.1.254

Vbrick Administrator Account

It is suggested that a vbrick administrator account is created for loading the software. To add a user run the following commands:

adduser vbrick = create user account vbrick

passwd vbrick = set password for vbrick user account (pw = vbrick1)



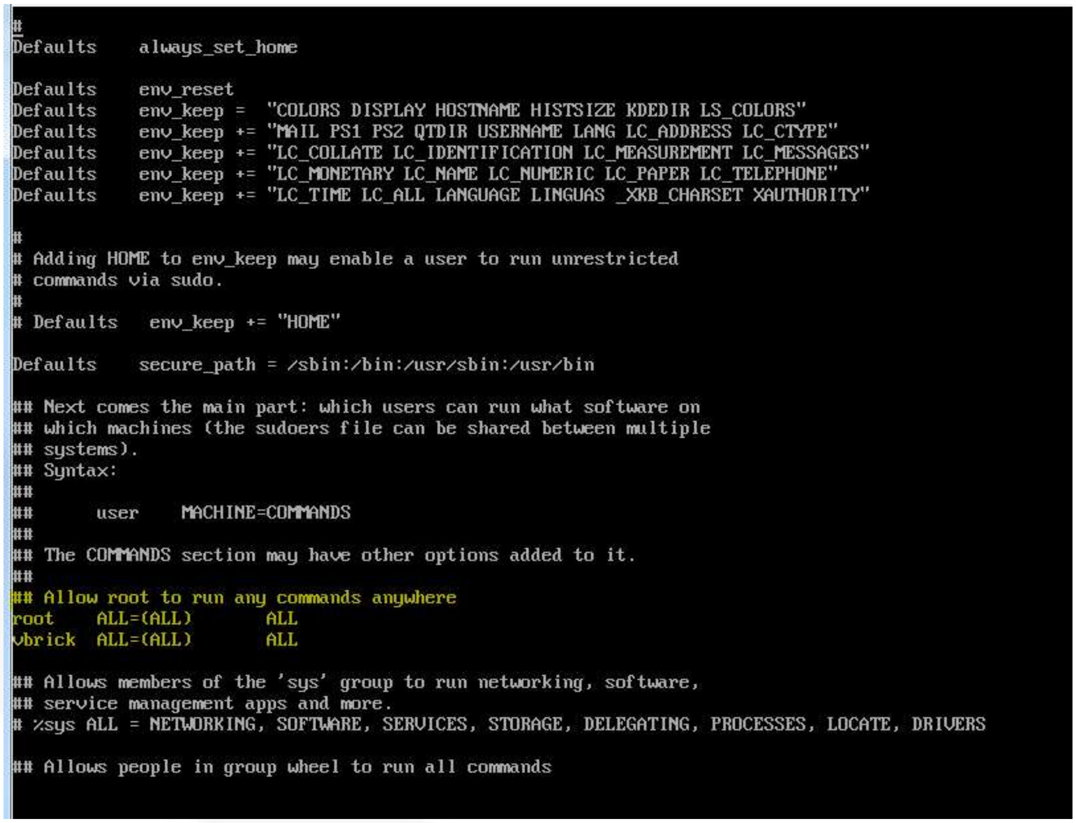
```
[root@Unknown-08-00-27-2b-76-b0 ~]# adduser vbrick
[root@Unknown-08-00-27-2b-76-b0 ~]# passwd vbrick
Changing password for user vbrick.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
```

Provide sudo privilages to the Vbrick account

The visudo command is a safe and secure way of editing the /etc/sudoers file on UNIX and Linux systems. Since the sudoers file determines which users can run administrative tasks, those requiring superuser privileges, it is a good idea to take some precautions when editing it, and that's what visudo does.

Run visudo at a command prompt and add:

```
        vbrick      ALL=(ALL)      ALL   ## Allow vbrick to run any commands anywhere like the root account.
```

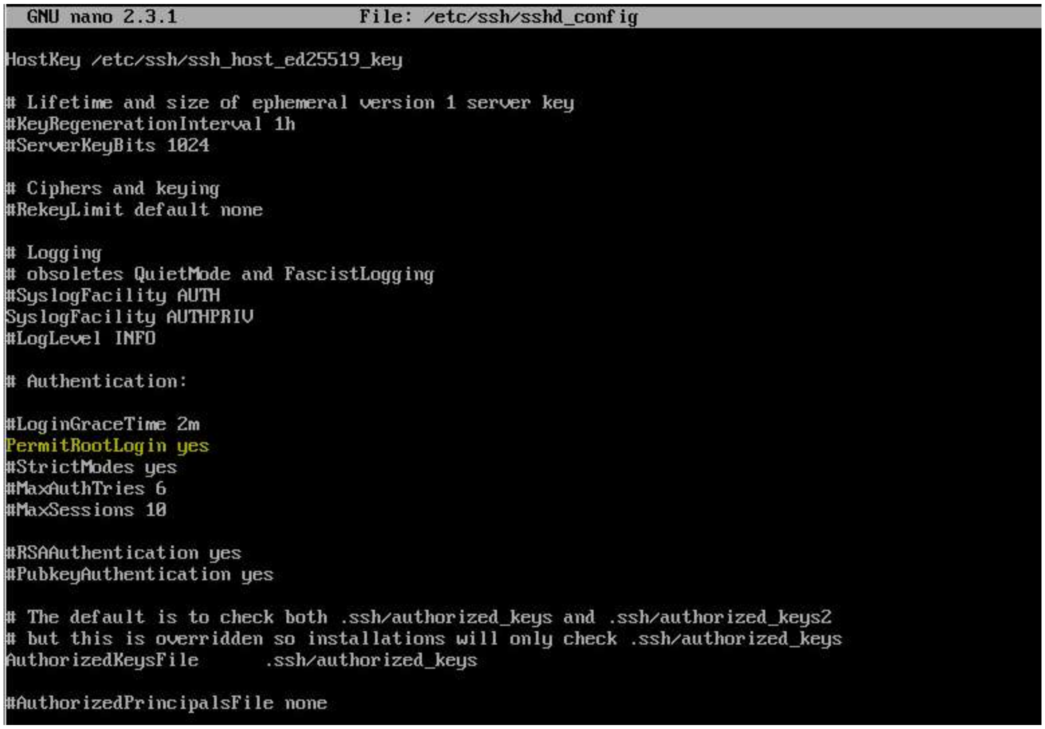


```
#
Defaults    always_set_home

Defaults    env_reset
Defaults    env_keep =  "COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS"
Defaults    env_keep += "MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE"
Defaults    env_keep += "LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES"
Defaults    env_keep += "LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE"
Defaults    env_keep += "LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY"

#
# Adding HOME to env_keep may enable a user to run unrestricted
# commands via sudo.
#
# Defaults   env_keep += "HOME"

Defaults    secure_path = /sbin:/bin:/usr/sbin:/usr/bin

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
vbrick  ALL=(ALL)       ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
```

Reboot the server after adding the vbrick account to the visudo file. Run the command “sudo su –“ and ensure that the vbrick account can do an “ls – la / root” (Accessing the root folder is normally only accessible to the root user).

ENABLING SSH

To be able to transfer files needed for the install you will need to run Authentication on the Linux server. Change the ***PermitRootLogin*** of the sshd_config file to ***yes*** and restart the SSH server (service sshd restart).

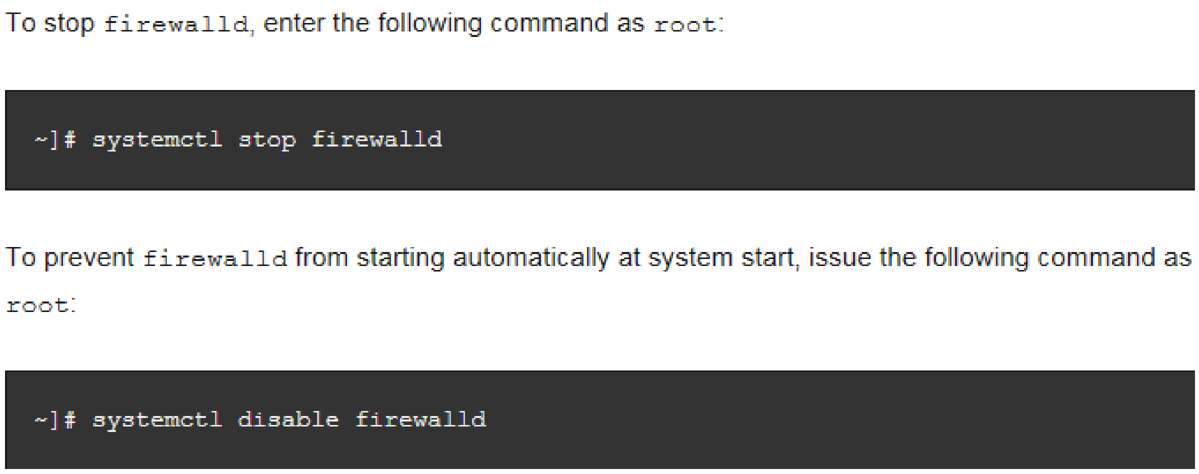


```
  GNU nano 2.3.1                  File: /etc/ssh/sshd_config

HostKey /etc/ssh/ssh_host_ed25519_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 1h
#ServerKeyBits 1024

# Ciphers and keying
#RekeyLimit default none

# Logging
# obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#RSAAuthentication yes
#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none
```

DISABLING THE FIREWALL ON THE SERVER

When deploying the Linux OS, avoid doing a minimal install. You might need to add in some files so that you can edit files or install software if you do a minimal install. You will need to find the Yum command to install the software packages needed for the commands that you are trying to run such as Nano vs using the VI editor. "***yum install nano***" is the Red Hat command that will load the package to use the Nano editor.

It is suggested that you temporarily turn off the Linux server's firewall



To stop `firewalld`, enter the following command as `root`:

```
~]# systemctl stop firewalld
```

To prevent `firewalld` from starting automatically at system start, issue the following command as `root`:

```
~]# systemctl disable firewalld
```

TRANSFERRING THE TAR FILE

Transfer the vbrick-packageinstall-7.22_XX.tar software to all servers either with the SCP Utility or with WinSCP.

NOTE: Servers MUST be installed in the following order:

1) HAProxy
2) Elastic 1
3) Elastic 2 (If Dual Node)
4) Mongo 1
5) Mongo 2 (If Dual Node)

The installation package no longer asks if you are installing the primary Elastic server or the secondary server, it is assumed that you are installing the system in order.

UPGRADING REV

When upgrading an On-Premise Rev system there are several things that you need to understand prior to the upgrade. Below are background questions that need to be asked prior to upgrading the customers system.

Upgrades can only be made from one on-premise release to the next on-premise release. Cumulative upgrades are not possible. The upgrade path is as follows:

7.6 -> 7.7 -> 7.9 -> 7.12 -> 7.15 -> 7.18 -> 7.22

For example, when running Vbrick Rev 7.9, the system must first be upgraded to Vbrick Rev 7.12 and tested. Only after this is done may the system be upgraded from Vbrick Rev 7.12 to 7.15 and so forth…

Background Questions

- Rev Configuration
  - How many total HW servers, if any?
  - How many run time VMs?
  - How many mongo VMs?
  - How many Elastic Search VMs?
- Is Vbrick's HA Proxy used or is there a customer load balancer?
- Was a HA Proxy used to install the initial system? If so, is it still in use? Disabled? Or was it used and deleted?
- What Linux is used for Rev? Was it installed using the Vbrick provided ISO (Ubuntu) or is it a customer provided Red Hat or other Linux version?
- What are the maintenance window hours to perform the upgrade activity?
- Is staff available to download all the required upgrade files before starting an upgrade session as this is one of the required prerequisites?
- Is there currently any customization development on Rev (note that this must be indicated so we can understand what impacts newer releases may have to this planned upgrade)?
- Can SSH client, Putty and WINSCP be loaded on the Computer that is being used for the upgrade?
- What user was used to install the software on the Rev server? Is that account still available?

Customer Prerequisites prior to Upgrade

7.9 to 7.12

- Are the Elastic Search / Mongo servers allowed to access the internet? (this is because there are Ubuntu OS upgrades that will need access to the internet to download files for the upgrade). Rev 7.12 Linux components no longer supports Ubuntu 12.04. So if you are using Ubuntu 12.04, you will have to upgrade to Ubuntu 14.04 to proceed with the upgrade.
- Note that new License files will be needed for Rev and will need to be requested from Vbrick Support.
- The location that the Analytics are processed moves from Mongo to Elastic. To ensure that the old data is saved you will need to ensure that you run the **AnalyticsExporter.exe** command on the Primary Mongo server. If this step is missed in the instructions then the old data will be lost.

7.12 to 7.15

- Ensure that the .NET framework update provided in the patch fully installs. The following itmes are included in the patch:
  - KB2919355
  - KB2919442
  - KB2932046
  - KB2934018
  - KB2937592
  - KB2938439
  - KB2959977

7.15 to 7.18

- ElasticSearch indices should be checked before any 7.18 upgrade. Only indices that begin with “rev”, “audit” and “analytics” should be located on the ElasticSearch server. It is important that the server only have these indices as the 7.18 upgrade might fail. Indices other than “rev”, “audit” and “analytics” might be on the server if the customer is using the ElasticSearch servers for applications other than rev. It is against Vbrick policy to use the ElasticSearch servers for anything other than Rev so deleting the
- NOTE – Please contact Vbrick Support prior to performing this upgrade to obtain a copy of a database script which must be run at the completion of this upgrade. This script is NOT part of the standard upgrade scripts provided for this upgrade and must be obtained separately.

7.18 to 7.22

- Beginning with release 7.22, Vbrick has dropped direct Operating System support. In previous releases, an ISO-based installer could be used to deploy hardware or virtual machines with Ubuntu 14.04 and all the packaging necessary to support the desired role for that device. For 7.22 Vbrick will no longer distribute the ISO image, instead we're releasing a Package Installer that works similar in many ways to previous installers but provides support for both Ubuntu 14.04 and Red Hat Enterprise Server 7. The change in installers allows Enterprise customers to favor their own machine deployments.

Rev On-Prem to Cloud Migration

Our On-Prem to Cloud Migration Requires Preparation on both the customer’s network as well as the Vbrick Cloud. Below is an outline of the requirements for the On-Prem to Cloud Migration:

Design (estimated 1-2 weeks in duration)

- Solution Design Document (SDD)
- Site Checklist / Contact Information
- Implementation Plan Signoff
- Streaming Configuration (Dual Homing to On Prem and Cloud Rev)
- Design Signoff - Complete

Customer Infrastructure Preparation (estimated 1-2 weeks in duration)

- URL assignments for Streaming
- Change Order Input and Approval
- Resource / Personnel Task Assignments
- Site Readiness-

Initial Rev Cloud Infrastructure Implementation (estimated 2-3 weeks in duration)

- REV Cloud Configuration
- Temporary DME Configuration (note that a DME cannot be dual homed to both Rev On Prem and Cloud at the same time)
- REV Environment and Local Streaming Configuration
- Configure any necessary workflows that mirror On Prem environment
- Test Rev Cloud Solution (with 1 temporary DME)

- Configure Streams from TCS / VC Gateway
- Content Migration

Production Rev Cloud Infrastructure Implementation (estimated < week in duration)

- Integrate Production DMEs to Rev Cloud (Rev On Prem integration ceases at that point)
- Configure new streaming on production DMEs
- Test Rev Cloud Production Solution (unit testing followed by event testing in increased scale)

Note that the backup plan in the event of Rev Cloud Issues is to revert DMEs back to Rev on prem integration.

How to obtain Software Licenses

Certain version of Rev for may require new license files for upgrades. Please email support@vbrick.com to obtain a new license file prior to upgrading the system.

Slide Delivery (Cloud)

This feature is available for Rev Cloud customers only. Static files (such as webcast slides, HTML, CSS, images, JavaScript) are delivered securely via AWS Cloudfront CDN. By default, this feature is ON for new Cloud customers starting with Rev 7.23 and OFF for pre-existing customers. Contact your Vbrick representative to find out if this feature is turned on for your Rev instance and/or to request that it be turned on.

If the customer has implemented whitelisting to access Rev, the following URLs must be added to the whitelist for this feature to work properly.

- media.us.vbrickrev.com and static.us.vbrickrev.com if hosted in Vbrick's North American data center
- media.eu.vbrickrev.com and static.eu.vbrickrev.com if hosted in Vbrick's EU data center
- media.au.vbrickrev.com and static.au.vbrickrev.com if hosted in Vbrick's EU data center

When testing live webcasts, make sure to test with slides to ensure proper slide delivery and visibility.

DME Implementation (On-premises or Cloud)

Overview

This guide does not give the installation steps for DME. It summarizes the best practices that VBrick teams follow while installing Rev. Please view the implementation documents that are available online and in the Vbrick website customer/partner portal.Please refer to the Appendix of this document for more links to these documents.

Architecture and Design

DME ARCHITECTURE OVERVIEW

The Rev H.264 Distributed Media Engine (DME) simplifies delivery of high definition video and other rich media content across multi-site enterprises and campus environments. The DME accepts multiple H.264 media streams from multiple central sites and redistributes that content to diverse endpoints including PCs/MACs, mobile phones and televisions/ monitors. This one, integrated platform optimizes WAN bandwidth use, simplifies endpoint support and offers local storage of centrally managed content.

The DME also provides both live and VOD content caching, storage, transrating, transmuxing, and serving to ensure that stored content is delivered from a DME as close to the end user as possible. The DMEs corporate together using a set of technologies (the DME Mesh) for sharing and delivering content most effectively.

Depending upon your use cases and network topology, the DME can be deployed at a central location, to support transmuxing or transrating, or at remote locations to support distribution. It is a single, integrated platform providing media redistribution, media transformation and Video on Demand content storage.

For more details, please refer to the DME Administration guide (based on DME Version) for a complete description of features and functions.

In terms of deployment, the DME can be delivered as a hardware appliance (sold directly from Vbrick, or through a partner like Cisco) or, more commonly, as a virtual appliance. In all cases, the DME is provided with an underlying Linux OS that is a highly customized and secured. No direct shell access is provided, as this is a hardened system.

Please refer to the DME Release Notes (based on DME Version) for specific information on supported virtual hosts environments, versions, as well as VM sizing information per license level (e.g., 7530, 7550, 7570).

REDUNDANCY / HIGH AVAILABILITY

It is possible to use Rev Zoning logic for High Availability. The directing and redirecting of viewers is based on source (DMEs) status in Rev.

Inside a Certain Zone

Rev makes it possible to include multiple DMEs in the same zone. Once this is configured properly, viewers who request access to the video content will be directed to the multiple DMEs, in a sequential “round robin” fashion; so the DMEs will be sharing the load, without the need for additional load balancers.

This solution is especially useful if multiple DMEs are deployed in a specific site and it is possible for viewers to reach all these DMEs without engaging significant WAN resources.

Caution: If multiple formats are used for video distribution (i.e. Multicast and Unicast HLS), the DMEs should be configured to serve all the video formats that are required for that particular group of viewers.

Using the "Parent / Child" zoning feature

It is also possible to create a "Parent / Child" zoning structure.

With such a structure in place, if the DME in a "Child" zone becomes unavailable, the viewers who are requesting streams from inside that "Child" zone will be automatically directed to the video sources in the assigned "Parent" zone.

The system allows multiple levels of "Parent / Child" relationship (i.e. if Zone-3 is the "Parent" of Zone-2 and Zone-2 is the "Parent" of Zone-1, the logic will follow the multiple layers, if needed.)

Caution: The "Parent / Child" zoning structure should be designed and built keeping in mind the fact that the video sources in the different zones may be on a different LAN segments, therefore it is important to take into account the bandwidth availability on the connection(s) between the respective LAN segments.

Note: As mentioned above, the viewers' direct / redirect logic is based on DME status in Rev. A redirect will happen if a certain DME becomes unresponsive ("Off Line" state in Rev). It is also possible to manually put a DME in an "Inactive" state in Rev, in order to trigger (or test) the operation of the redirect logic.

CUSTOMER PROVIDED LOAD BALANCER

If physical (external) load balancers are desired, it is Customer's responsibility to provides and configure the respective load balancers. The VBrick PS team can offer some guidelines, but will not be responsible for configuring or ensuring the proper operation of these devices.

Implementation

DME STAGING AND INITIAL SETUP

Intended Audience

This setup guide is intended for IT Professionals with networking skills and working knowledge of VMware ESXi and vSphere environments.

A general understanding of enterprise streaming and familiarity with the VBrick suite of enterprise streaming products would be beneficial

Prerequisites

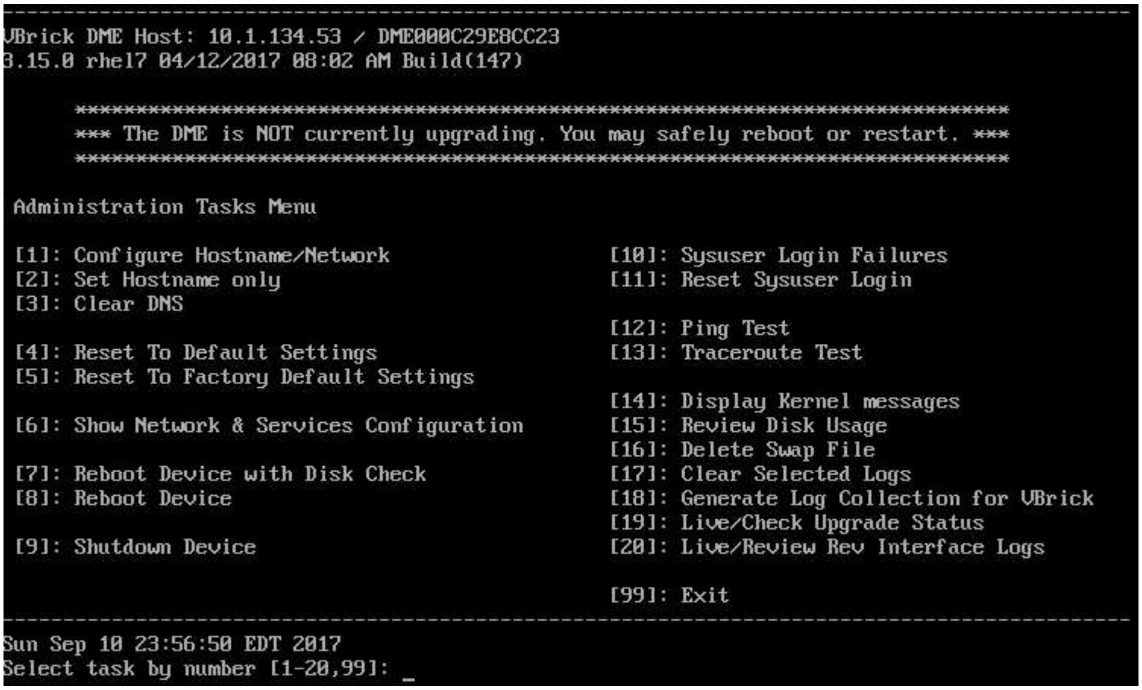
- Pre-staging and IP information reserved for the DME device to be deployed.
- Host platform meeting minimum VBrick DME deployment specification available on VMware ESXi platform.
- VBrick DME OVA file.
- API Key created on VBrick REV Portal for dedicated DME deployment.
  Note: When Deploying a virtualized DME Large, additional configuration may be required to achieve maximum throughput if the following condition applies

- Physical server with ESXI OS hosting DME has four multiple GigE ports to the same VLan. (The Cisco UCS server designate for DME-L includes a quad Gig NIC card that must be connected)
- DME has appropriate license for DME Large (7570)
  The proper setup must have four separate VSwitch with four port group which each port group associated to each vswitch. Only 1 vmnic should be assigned to each vswitch. When initially deploying the DME OVA, the default template includes 4 virtual nics which each nic should be set to the four different port groups. After the initial IP address is set (see section Configure DME Network Settings), log into the web UI of the DME, navigate to Network Settings, and enable Load Sharing on Interface 2,3,4 (Important do not enable these setting if you are not setting up the DME with multiple physical NICs). This will reboot the DME and will be configured for software NIC load balancing.

Initial Configuration

a. Deploy the DME VM

   i. Using VMware vSphere client, connect and login to the ESXi management interface.
   ii. Deploy the DME VMware OVA image file on the physical host.
   iii. Power on the DME VM.
   iv. Using VMware vSphere client, open the DME's console and login with the default credentials.
   v. The system will display the Administrative Tasks menu



```
-----------------------------------------------------------------------------------------------
VBrick DME Host: 10.1.134.53 / DME000C29E8CC23
3.15.0 rhel7 04/12/2017 08:02 AM Build(147)

      *****************************************************************************
      *** The DME is NOT currently upgrading. You may safely reboot or restart. ***
      *****************************************************************************

 Administration Tasks Menu

 [1]: Configure Hostname/Network                  [10]: Sysuser Login Failures
 [2]: Set Hostname only                           [11]: Reset Sysuser Login
 [3]: Clear DNS
                                                  [12]: Ping Test
 [4]: Reset To Default Settings                   [13]: Traceroute Test
 [5]: Reset To Factory Default Settings
                                                  [14]: Display Kernel messages
 [6]: Show Network & Services Configuration       [15]: Review Disk Usage
                                                  [16]: Delete Swap File
 [7]: Reboot Device with Disk Check               [17]: Clear Selected Logs
 [8]: Reboot Device                               [18]: Generate Log Collection for VBrick
                                                  [19]: Live/Check Upgrade Status
 [9]: Shutdown Device                             [20]: Live/Review Rev Interface Logs

                                                  [99]: Exit
-----------------------------------------------------------------------------------------------
Sun Sep 10 23:56:50 EDT 2017
Select task by number [1-20,99]: _
```

b. Select option 5 - *Reset to Factory Default Settings*.

c. Confirm selection and wait for the server to reboot.

Configure DME Network Settings

i. Using VMware vSphere client, access the DME's console and login with the default credentials.

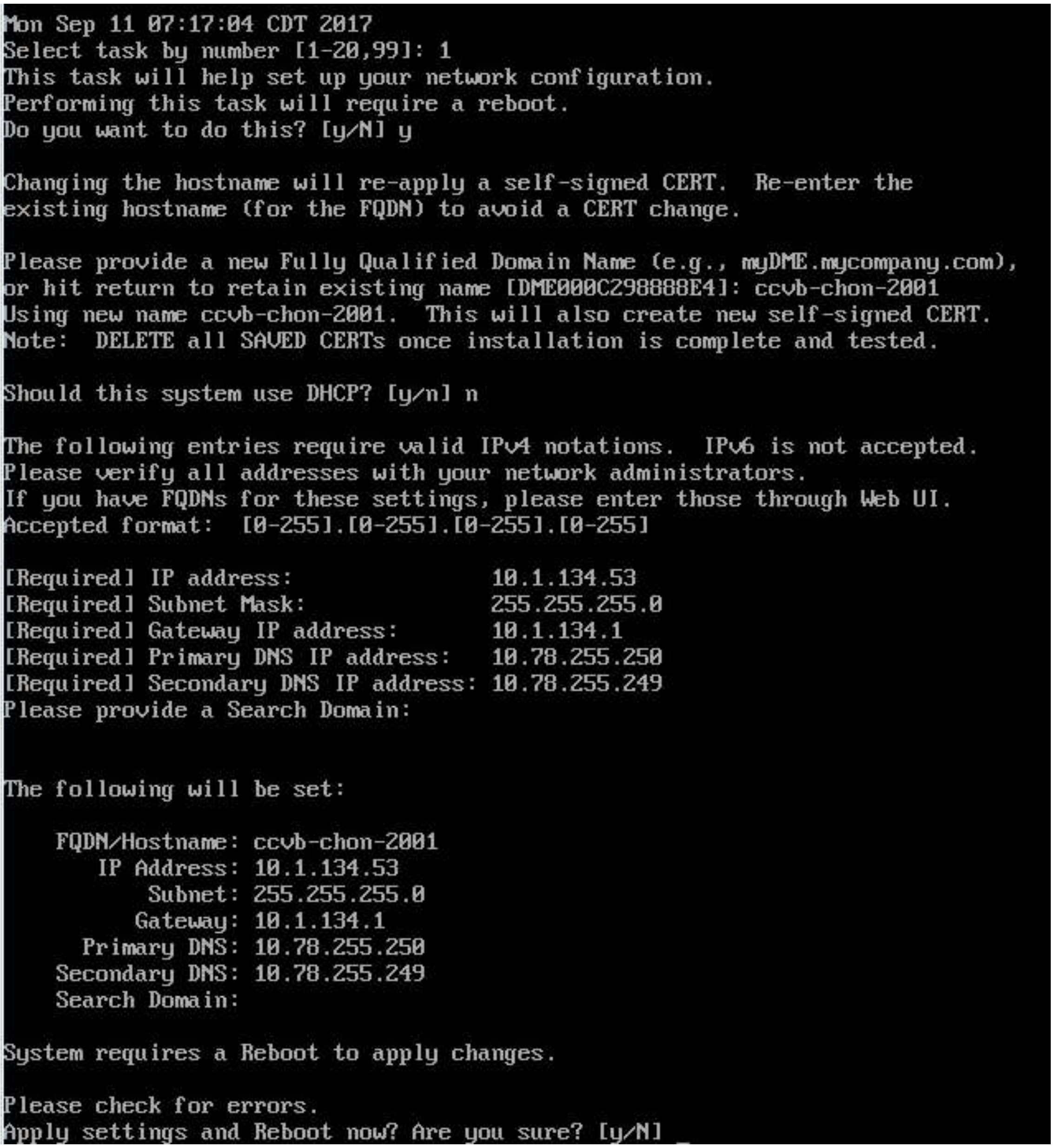
ii. From Administrative Tasks menu select ***Option 1 – Configure Network*** to configure the network settings.

iii. Follow the console prompts to set the IP information:

Select **y** to confirm that you want to change the IP settings

- Enter hostname / FQDN
- Select n to disable DHCP
- Enter the IP address
- Enter Subnet Mask
- Enter Default Gateway
- Enter Primary DNS
- Enter Secondary DNS
- Enter search domain

Select **y** to apply settings and reboot

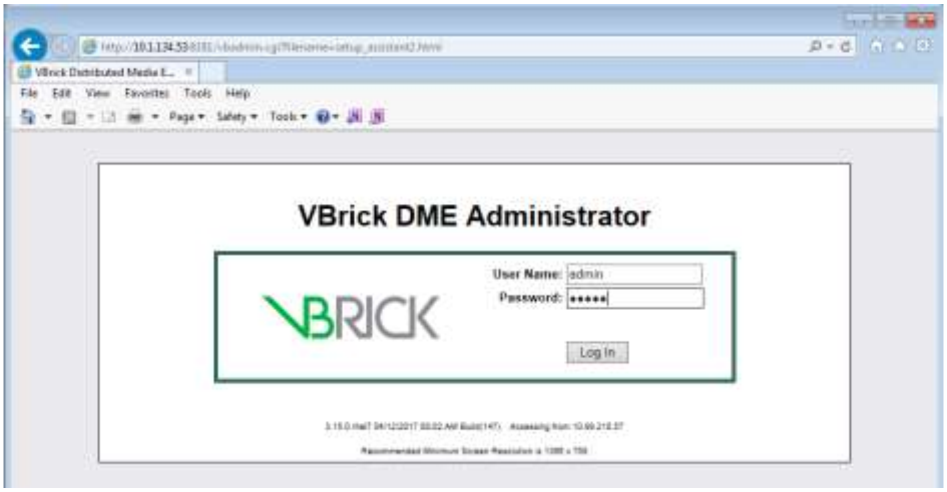


```
Mon Sep 11 07:17:04 CDT 2017
Select task by number [1-20,99]: 1
This task will help set up your network configuration.
Performing this task will require a reboot.
Do you want to do this? [y/N] y

Changing the hostname will re-apply a self-signed CERT.  Re-enter the
existing hostname (for the FQDN) to avoid a CERT change.

Please provide a new Fully Qualified Domain Name (e.g., myDME.mycompany.com),
or hit return to retain existing name [DME000C298888E4]: ccvb-chon-2001
Using new name ccvb-chon-2001.  This will also create new self-signed CERT.
Note:  DELETE all SAVED CERTs once installation is complete and tested.

Should this system use DHCP? [y/n] n

The following entries require valid IPv4 notations.  IPv6 is not accepted.
Please verify all addresses with your network administrators.
If you have FQDNs for these settings, please enter those through Web UI.
Accepted format:  [0-255].[0-255].[0-255].[0-255]

[Required] IP address:              10.1.134.53
[Required] Subnet Mask:             255.255.255.0
[Required] Gateway IP address:      10.1.134.1
[Required] Primary DNS IP address:  10.78.255.250
[Required] Secondary DNS IP address: 10.78.255.249
Please provide a Search Domain:


The following will be set:

    FQDN/Hostname: ccvb-chon-2001
       IP Address: 10.1.134.53
           Subnet: 255.255.255.0
          Gateway: 10.1.134.1
      Primary DNS: 10.78.255.250
    Secondary DNS: 10.78.255.249
    Search Domain:

System requires a Reboot to apply changes.

Please check for errors.
Apply settings and Reboot now? Are you sure? [y/N] _
```

Obtain and Apply DME License

After the DME reboots, use a web browser to navigate to the VBrick DME Administrator Interface using the IP address of the DME configured in previous step: e.g., http://<DME-IP>

Note: If the login prompt does not come up right away, try again adding :8181 at the end of the URL.


http://10.1.134.53:8181/vbadmin.cgi?filename=setup_assistant2.html
VBrick Distributed Media E...
File Edit View Favorites Tools Help
Page Safety Tools
Log In

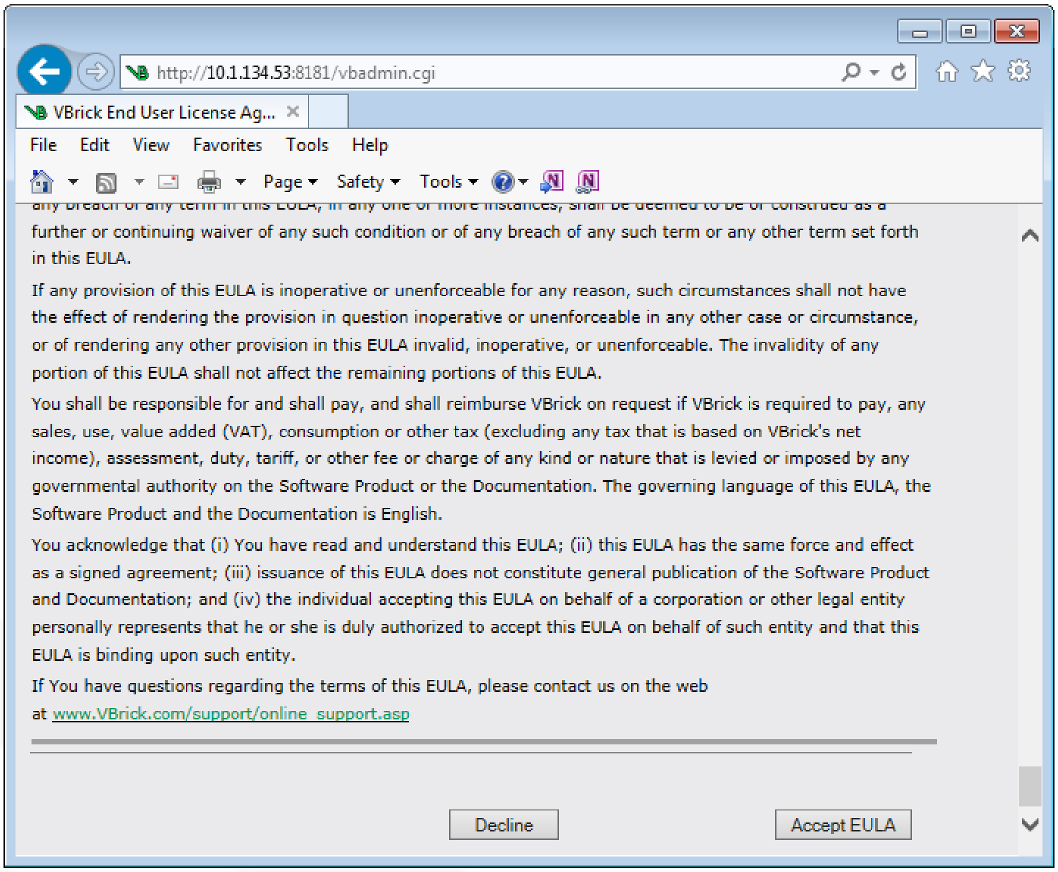
VBrick DME Administrator

User Name: admin
Password: •••••

3.15.0 rhel7 04/12/2017 03:02 AM Build(147) Accessing from: 10.99.215.37

Recommended Minimum Screen Resolution is 1280 x 768

1. If prompted, click the button to accept the EULA:


http://10.1.134.53:8181/vbadmin.cgi
VBrick End User License Ag...
File Edit View Favorites Tools Help
Page Safety Tools
Decline
Accept EULA

any breach of any term in this EULA, in any one or more instances, shall be deemed to be or construed as a further or continuing waiver of any such condition or of any breach of any such term or any other term set forth in this EULA.

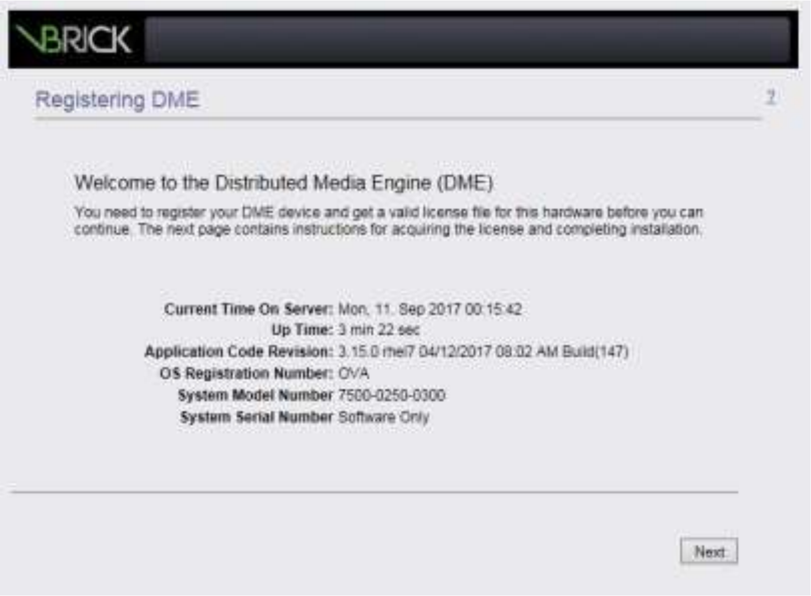
If any provision of this EULA is inoperative or unenforceable for any reason, such circumstances shall not have the effect of rendering the provision in question inoperative or unenforceable in any other case or circumstance, or of rendering any other provision in this EULA invalid, inoperative, or unenforceable. The invalidity of any portion of this EULA shall not affect the remaining portions of this EULA.

You shall be responsible for and shall pay, and shall reimburse VBrick on request if VBrick is required to pay, any sales, use, value added (VAT), consumption or other tax (excluding any tax that is based on VBrick's net income), assessment, duty, tariff, or other fee or charge of any kind or nature that is levied or imposed by any governmental authority on the Software Product or the Documentation. The governing language of this EULA, the Software Product and the Documentation is English.

You acknowledge that (i) You have read and understand this EULA; (ii) this EULA has the same force and effect as a signed agreement; (iii) issuance of this EULA does not constitute general publication of the Software Product and Documentation; and (iv) the individual accepting this EULA on behalf of a corporation or other legal entity personally represents that he or she is duly authorized to accept this EULA on behalf of such entity and that this EULA is binding upon such entity.

If You have questions regarding the terms of this EULA, please contact us on the web at www.VBrick.com/support/online_support.asp

2. On the following page, click on ***Next***



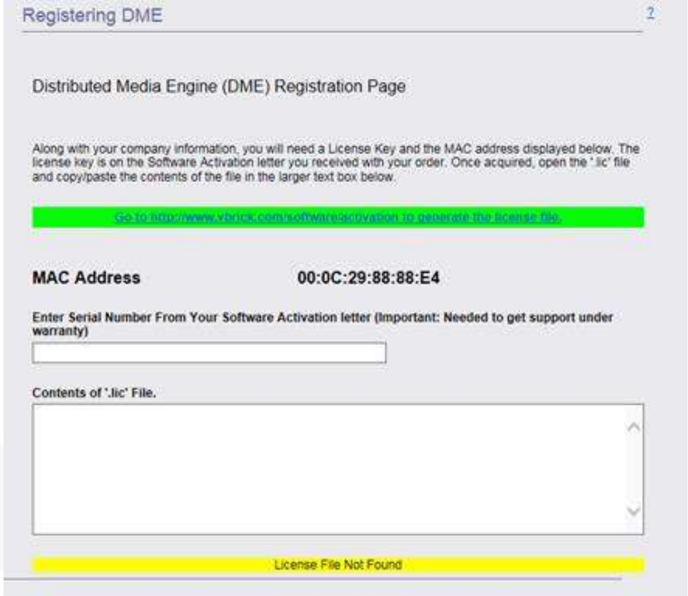
Registering DME

Welcome to the Distributed Media Engine (DME)

You need to register your DME device and get a valid license file for this hardware before you can continue. The next page contains instructions for acquiring the license and completing installation.

Current Time On Server: Mon, 11. Sep 2017 00:15:42
Up Time: 3 min 22 sec
Application Code Revision: 3.15.0 rhel7 04/12/2017 08:02 AM Build(147)
OS Registration Number: OVA
System Model Number 7500-0250-0300
System Serial Number Software Only

3. The DME will ask for a serial number and License file.



Registering DME

Distributed Media Engine (DME) Registration Page

Along with your company information, you will need a License Key and the MAC address displayed below. The license key is on the Software Activation letter you received with your order. Once acquired, open the '.lic' file and copy/paste the contents of the file in the larger text box below.

Go to http://www.vbrick.com/softwareactivation to generate the license file.

MAC Address **00:0C:29:88:88:E4**

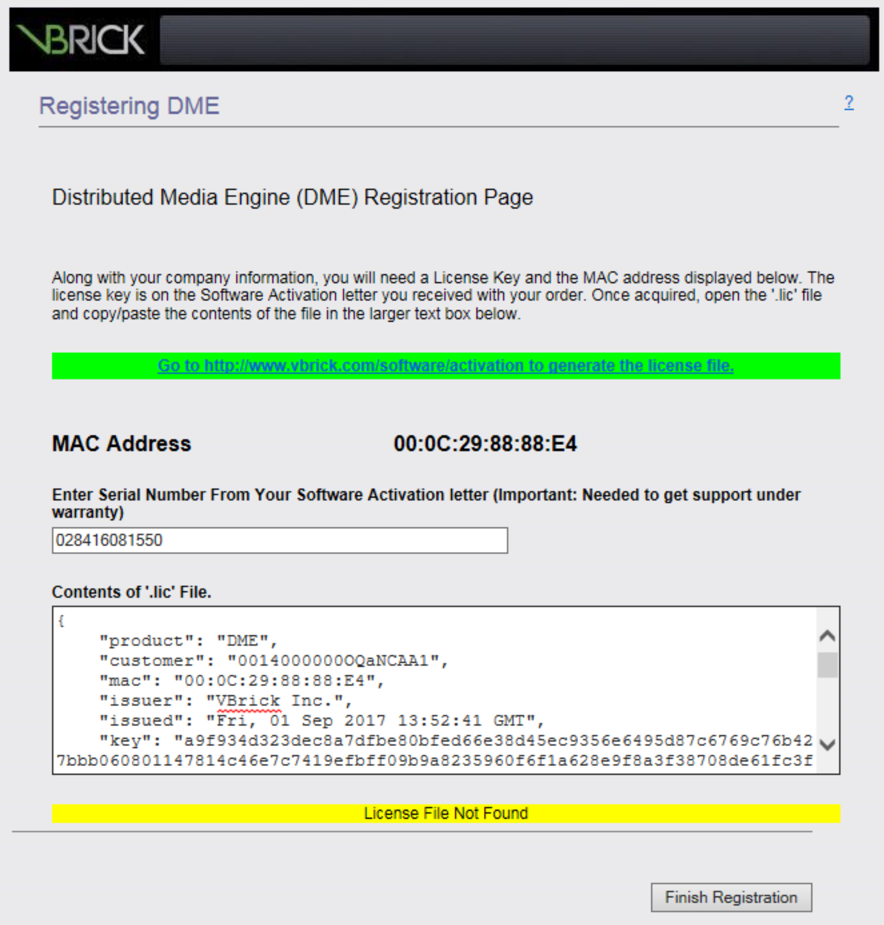
Enter Serial Number From Your Software Activation letter (Important: Needed to get support under warranty)

Contents of '.lic' File.

License File Not Found

4. Copy the MAC address displayed on the licensing screen.
5. Send email to VBrick Support support@vbrick.com , including the MAC address and required DME size (7570, 7550, 7530) to request the license file and the serial number.
6. The license file is normally delivered as an attached file, in TXT format.
   Note: If needed (or if a longer wait time is involved), it is OK to navigate away from the DME licensing page; or even close the browser window.

7. Once the serial number and license file have been received from VBrick Support, revert to the DME licensing page and paste the relevant data in to the appropriate fields.
   Note: Do not include any leading or trailing spaces with the Serial Number.
8. Open the license file in Notepad, select the entire text and paste in to the ***Contents of *.lic**** file box on the DME licensing page.



Registering DME

Distributed Media Engine (DME) Registration Page

Along with your company information, you will need a License Key and the MAC address displayed below. The license key is on the Software Activation letter you received with your order. Once acquired, open the '.lic' file and copy/paste the contents of the file in the larger text box below.

Go to http://www.vbrick.com/software/activation to generate the license file.

MAC Address **00:0C:29:88:88:E4**

Enter Serial Number From Your Software Activation letter (Important: Needed to get support under warranty)

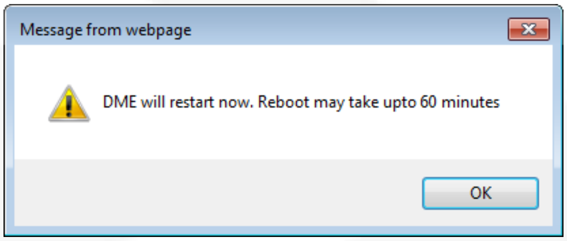
028416081550

Contents of '.lic' File.

```
{
    "product": "DME",
    "customer": "00140000000QaNCAA1",
    "mac": "00:0C:29:88:88:E4",
    "issuer": "VBrick Inc.",
    "issued": "Fri, 01 Sep 2017 13:52:41 GMT",
    "key": "a9f934d323dec8a7dfbe80bfed66e38d45ec9356e6495d87c6769c76b42
7bbb060801147814c46e7c7419efbff09b9a8235960f6f1a628e9f8a3f38708de61fc3f
```

License File Not Found

9. Click on ***Finish Registration*** to apply the licensing information.
10. At the prompt, click ***OK*** to reboot the DME.
    Note: Depending on the type of license, the system may take up to 60 minutes to build all the internal file structure of the server before boot up.

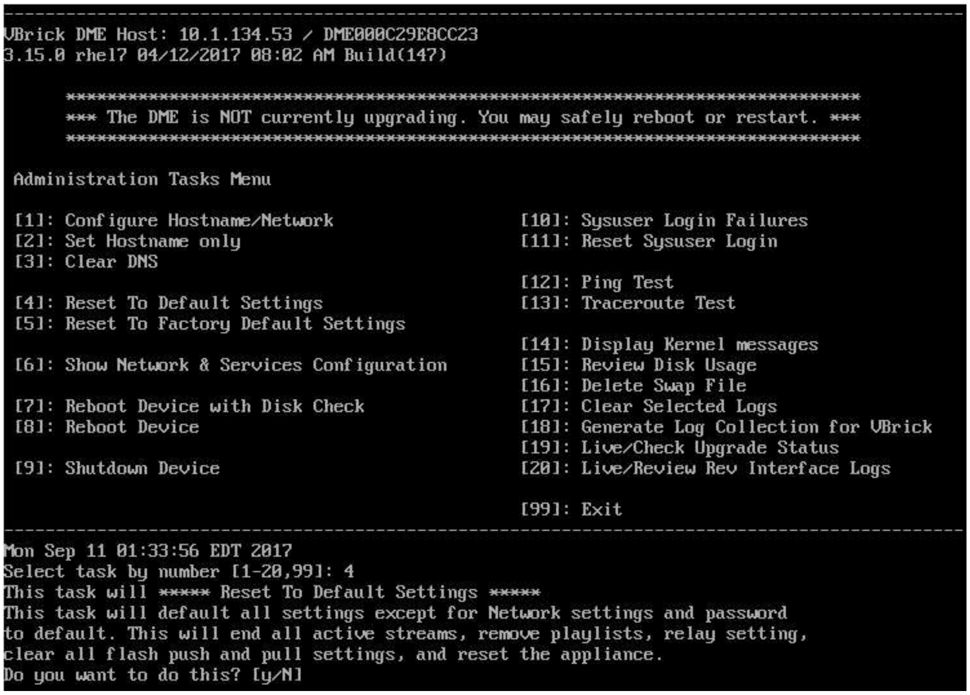


Message from webpage

DME will restart now. Reboot may take upto 60 minutes

Important: DO NOT interrupt this process (by forcing a “shut down” of the DME VM, or in any other way). This step is important for the future proper operation of the DME.

11. Once the DME has restarted, from VMware vSphere client, access the DME console and login with the default credentials.
12. From Administrative Tasks menu select ***Option 4 – Reset to Default Settings***.
    Note: The OVA image is based on DME 7530 (small). This step re-aligns machine configuration for the correct DME size, as directed by the license file (streams and bandwidth capabilities). Network settings and passwords remain unchanged.
13. Select y to confirm selection and wait for the server to reboot.



```
------------------------------------------------------------------------------------------------
VBrick DME Host: 10.1.134.53 / DME000C29E8CC23
3.15.0 rhel7 04/12/2017 08:02 AM Build(147)

      ******************************************************************************
      *** The DME is NOT currently upgrading. You may safely reboot or restart. ***
      ******************************************************************************

 Administration Tasks Menu

 [1]: Configure Hostname/Network                  [10]: Sysuser Login Failures
 [2]: Set Hostname only                           [11]: Reset Sysuser Login
 [3]: Clear DNS
                                                  [12]: Ping Test
 [4]: Reset To Default Settings                   [13]: Traceroute Test
 [5]: Reset To Factory Default Settings
                                                  [14]: Display Kernel messages
 [6]: Show Network & Services Configuration       [15]: Review Disk Usage
                                                  [16]: Delete Swap File
 [7]: Reboot Device with Disk Check               [17]: Clear Selected Logs
 [8]: Reboot Device                               [18]: Generate Log Collection for VBrick
                                                  [19]: Live/Check Upgrade Status
 [9]: Shutdown Device                             [20]: Live/Review Rev Interface Logs

                                                  [99]: Exit
------------------------------------------------------------------------------------------------
Mon Sep 11 01:33:56 EDT 2017
Select task by number [1-20,99]: 4
This task will ***** Reset To Default Settings *****
This task will default all settings except for Network settings and password
to default. This will end all active streams, remove playlists, relay setting,
clear all flash push and pull settings, and reset the appliance.
Do you want to do this? [y/N]
```

14. Record DME license information for future reference.

Host Environment: Review and Configure Additional Settings

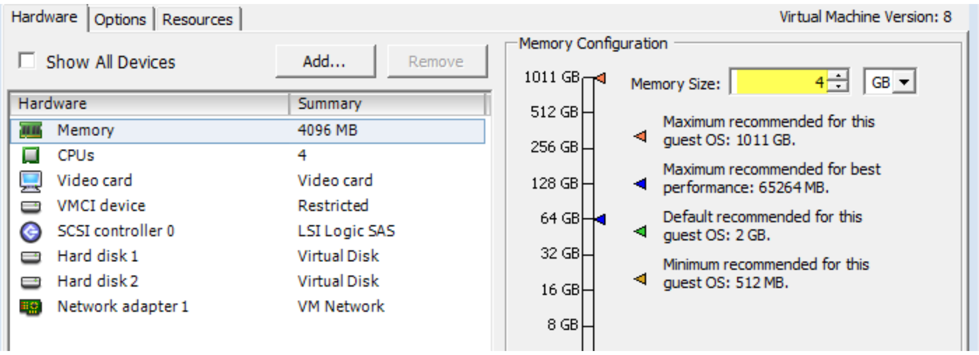
1. After the DME reboots, log in to the VBrick DME Administrator Interface: http://<DME-IP>
2. Turn off the DME: Configuration Menu | Maintenance | System Maintenance | System Shutdown, click Shutdown button.
3. Using the vSphere client, log in to the host environment and check the virtual server resource settings are correct for the deployed DME model:

DME	CPU Cores	Memory (GB)	Primary Partition (GB)	Secondary Partition (GB)	Network Interface	Operating System	Notes
Base Template	2	4	32	100*	4x1GB	RHEL7	OVA Default Settings see Note*
Small (7530)	4	4	32	100*	1x1GB	RHEL7	Max throughput - 250 Mb/s
Medium (7550)	8	16	32	100*	1x1GB	RHEL7	Max throughput - 500 Mb/s
Large (7570)	16	32	32	100*	4x1GB	RHEL7	Max throughput – 3.2 Gb/s

Note* All the OVF/Hyper-V loads use this footprint. Expand as needed after deployment.

For the most current specifications pleae consult the latest DME Release Notes.

The following screenshots are for reference only; the actual UI may look different and the size of the respective resources should match the requirements shown in the table above.



Hardware	Summary
Memory	4096 MB
CPUs	4
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Network adapter 1	VM Network

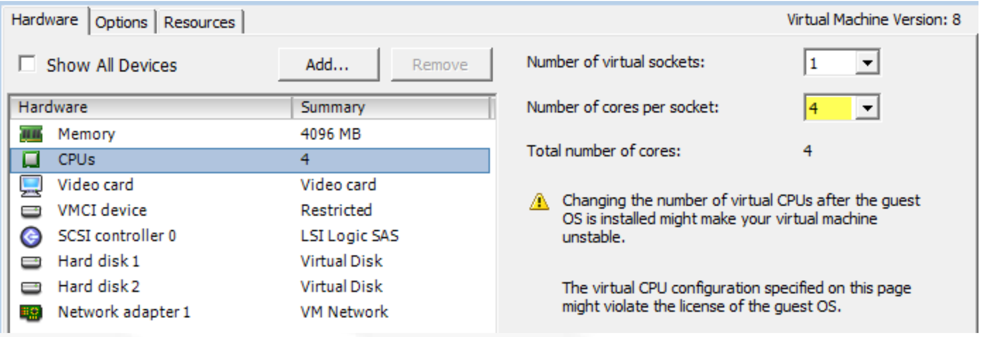
Memory Size: 4 GB

Maximum recommended for this guest OS: 1011 GB.

Maximum recommended for best performance: 65264 MB.

Default recommended for this guest OS: 2 GB.

Minimum recommended for this guest OS: 512 MB.



Hardware	Summary
Memory	4096 MB
CPUs	4
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Network adapter 1	VM Network

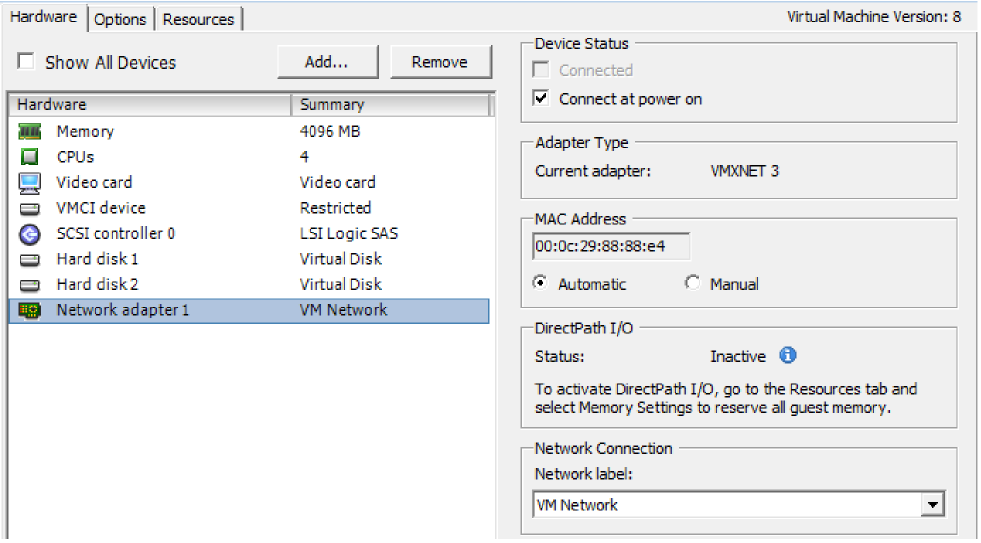
Number of virtual sockets: 1

Number of cores per socket: 4

Total number of cores: 4

⚠ Changing the number of virtual CPUs after the guest OS is installed might make your virtual machine unstable.

The virtual CPU configuration specified on this page might violate the license of the guest OS.



Virtual Machine Version: 8

□ Show All Devices

Hardware	Summary
Memory	4096 MB
CPUs	4
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Network adapter 1	VM Network

Device Status

□ Connected

☑ Connect at power on

Adapter Type

Current adapter: VMXNET 3

MAC Address

00:0c:29:88:88:e4

● Automatic ○ Manual

DirectPath I/O

Status: Inactive

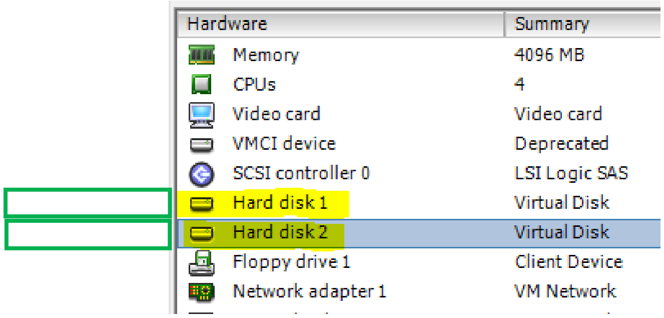
To activate DirectPath I/O, go to the Resources tab and select Memory Settings to reserve all guest memory.

Network Connection

Network label:

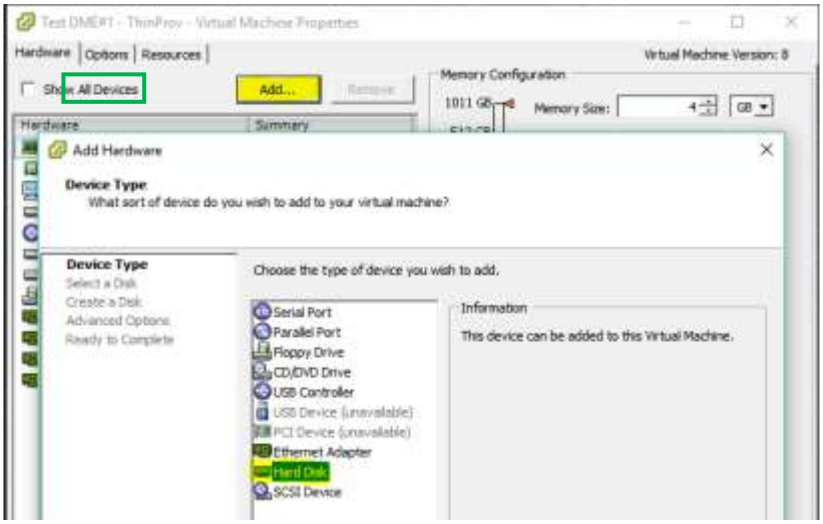
VM Network

<u>DO NOT resize any of the original virtual Hard Drives of the DME VM</u>. These appear as Hard disk 1 and Hard disk 2 and their sized are 32GB and 100GB, respectively. They must be left as they are.



Hardware	Summary
Memory	4096 MB
CPUs	4
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Floppy drive 1	Client Device
Network adapter 1	VM Network

In order to increase the available storage space on the DME, create additional Hard Drives on the VM.



Device Type
What sort of device do you wish to add to your virtual machine?

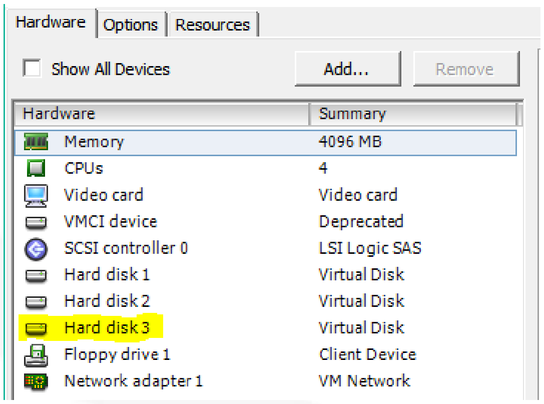
Choose the type of device you wish to add.

This device can be added to this Virtual Machine.

Once the additional Hard Disk has been created, proceed to the next steps.

Note: It is not imperative that you create the additional storage space right away after the DME has been deployed. Depending on the use case, DMEs may be able to operate properly, at least for a while, with the storage space available in the default setup. Hard drives can be added at a later time, on an as needed basis.

If you decidced to add a Hard Disk at this time, make sure that the operation completed successfully, before you proceed to the next step.

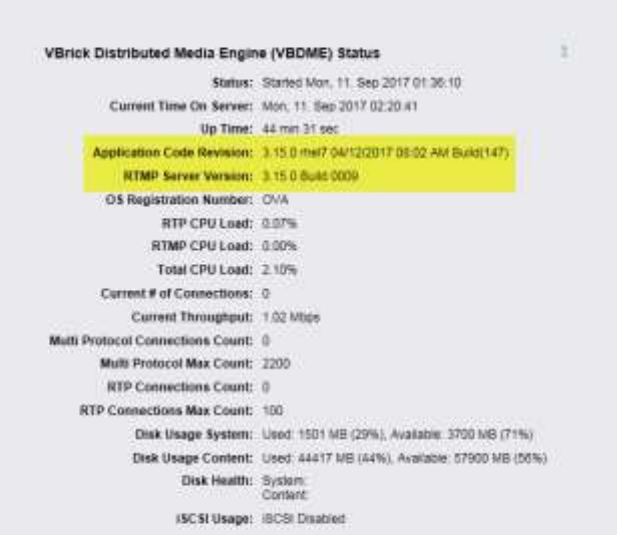


Hardware	Summary
Memory	4096 MB
CPUs	4
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Hard disk 3	Virtual Disk
Floppy drive 1	Client Device
Network adapter 1	VM Network

Once the virtual resources are set, Start the DME virtual machine.

Once the DME is operational (give it a couple of minutes to boot up), log back in to the VBrick DME Administrator Interface: <http://DME-IP> and check the following:

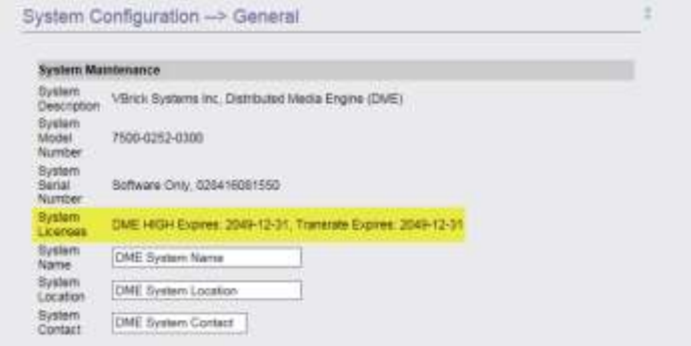
a. Software version is correct: Home



VBrick Distributed Media Engine (VBDME) Status

Status:	Started Mon, 11. Sep 2017 01:36:10
Current Time On Server:	Mon, 11. Sep 2017 02:20:41
Up Time:	44 min 31 sec
Application Code Revision:	3.15.0 rhel7 04/12/2017 08:02 AM Build(147)
RTMP Server Version:	3.15.0 Build 0009
OS Registration Number:	OVA
RTP CPU Load:	0.07%
RTMP CPU Load:	0.00%
Total CPU Load:	2.10%
Current # of Connections:	0
Current Throughput:	1.02 Mbps
Multi Protocol Connections Count:	0
Multi Protocol Max Count:	2200
RTP Connections Count:	0
RTP Connections Max Count:	100
Disk Usage System:	Used: 1501 MB (29%), Available: 3700 MB (71%)
Disk Usage Content:	Used: 44417 MB (44%), Available: 57900 MB (56%)
Disk Health:	System: Content:
iSCSI Usage:	iSCSI Disabled

b. License expiration: System Configuration | General | System Licenses

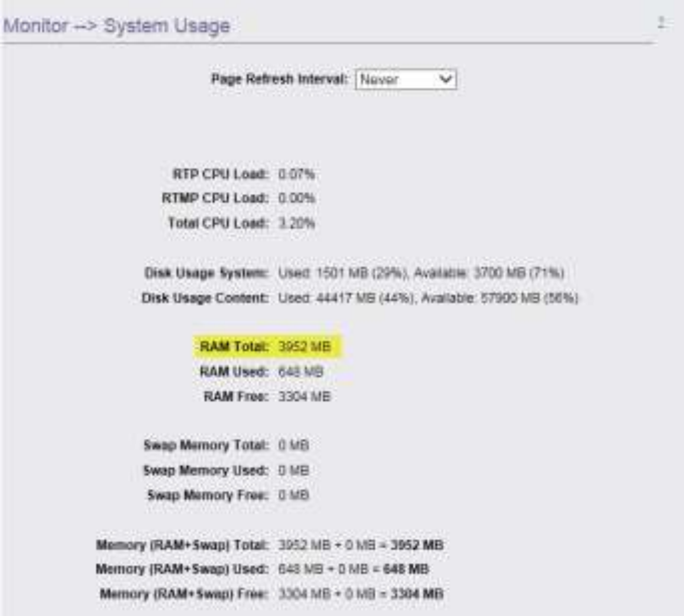


System Configuration --> General

System Maintenance

System Description	VBrick Systems Inc, Distributed Media Engine (DME)
System Model Number	7500-0252-0300
System Serial Number	Software Only, 028416081550
System Licenses	DME HIGH Expires: 2049-12-31, Transrate Expires: 2049-12-31
System Name	DME System Name
System Location	DME System Location
System Contact	DME System Contact

c. RAM is sufficient for DME model: Monitor | System Usage



Monitor --> System Usage

Page Refresh Interval: Never

RTP CPU Load: 0.07%
RTMP CPU Load: 0.00%
Total CPU Load: 3.20%

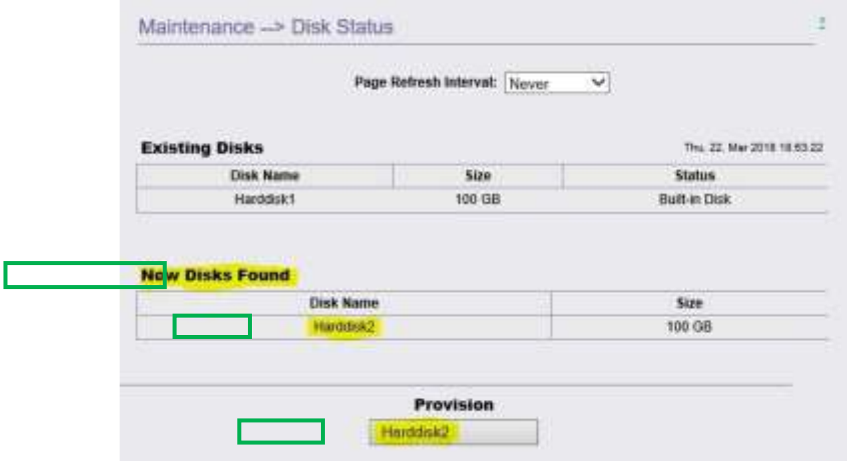
Disk Usage System: Used: 1501 MB (29%), Available: 3700 MB (71%)
Disk Usage Content: Used: 44417 MB (44%), Available: 57900 MB (56%)

RAM Total: 3952 MB
RAM Used: 648 MB
RAM Free: 3304 MB

Swap Memory Total: 0 MB
Swap Memory Used: 0 MB
Swap Memory Free: 0 MB

Memory (RAM+Swap) Total: 3952 MB + 0 MB = **3952 MB**
Memory (RAM+Swap) Used: 648 MB + 0 MB = **648 MB**
Memory (RAM+Swap) Free: 3304 MB + 0 MB = **3304 MB**

d. Disk size: Maintenance | Disk Status



Maintenance --> Disk Status

Page Refresh Interval: Never

Existing Disks

Thu, 22, Mar 2018 18:53:22

Disk Name	Size	Status
Harddisk1	100 GB	Built-in Disk

New Disks Found

Disk Name	Size
Harddisk2	100 GB

Provision

This page shows the “Existing Disks” (100GB “default” storage Hard Drive), as well as the “New Disks Found”, if one was added in the previous step. To make the new disk usable by the DME, click on the respective button in the “Provision” section.

The DME “Operating System” 32GB partition will not be displayed on this page.

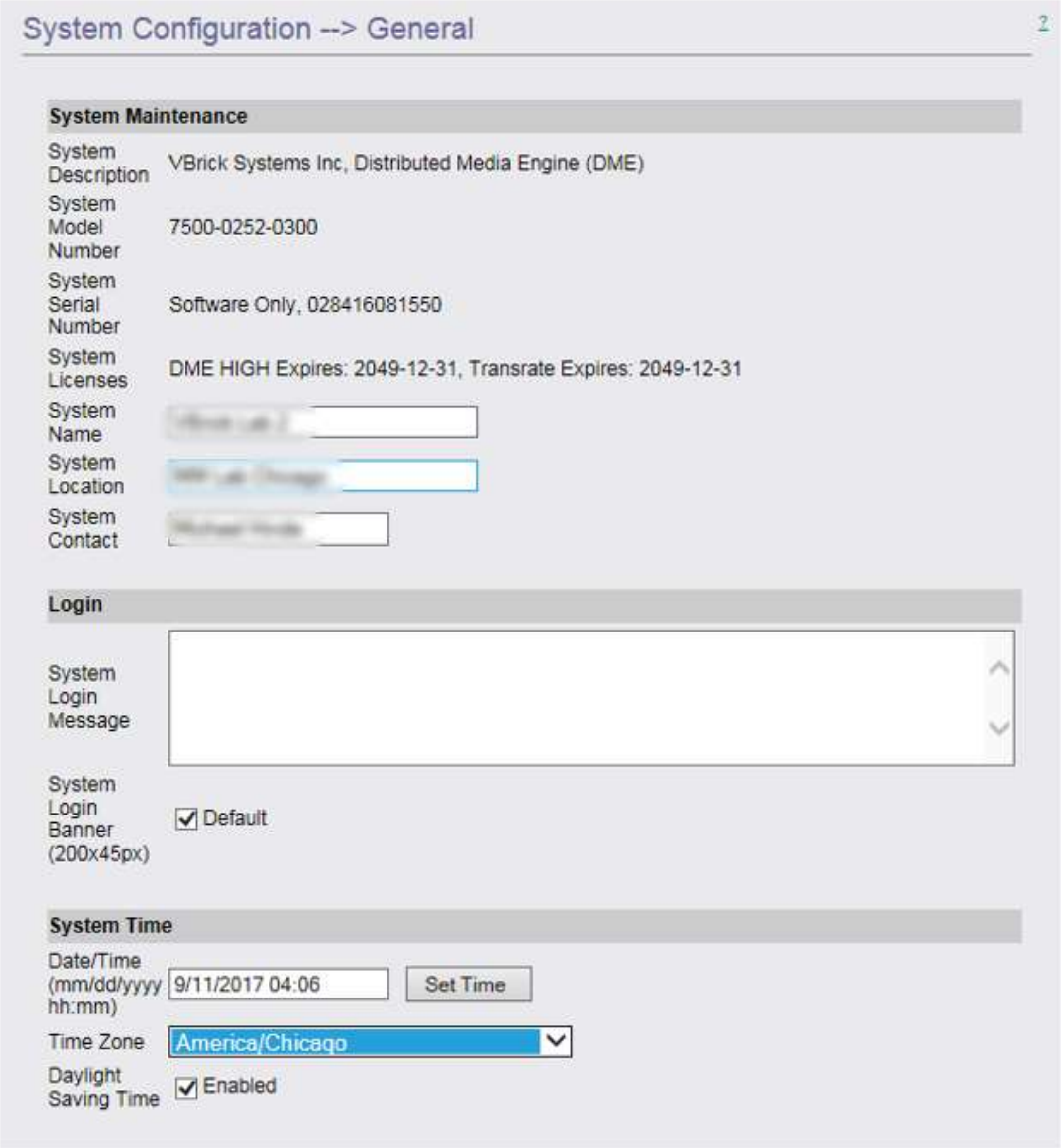
Note: Any vSphere configuration of the virtual host platform should be done with the DME shut down. To shut down the DME Maintenance | System Maintenance | System Shutdown

Finalize Initial DME Configuration

From VBrick DME Administrator Interface, navigate to:

- System Configuration / General and complete the following:
  - Add System Name, System Location and System Contact as required.

- Select required Time Zone setting
- Click the Apply button.



System Configuration --> General

System Maintenance

System Description: VBrick Systems Inc, Distributed Media Engine (DME)

System Model Number: 7500-0252-0300

System Serial Number: Software Only, 028416081550

System Licenses: DME HIGH Expires: 2049-12-31, Transrate Expires: 2049-12-31

System Name: [redacted]

System Location: [redacted]

System Contact: [redacted]

Login

System Login Message:

System Login Banner (200x45px): ☑ Default

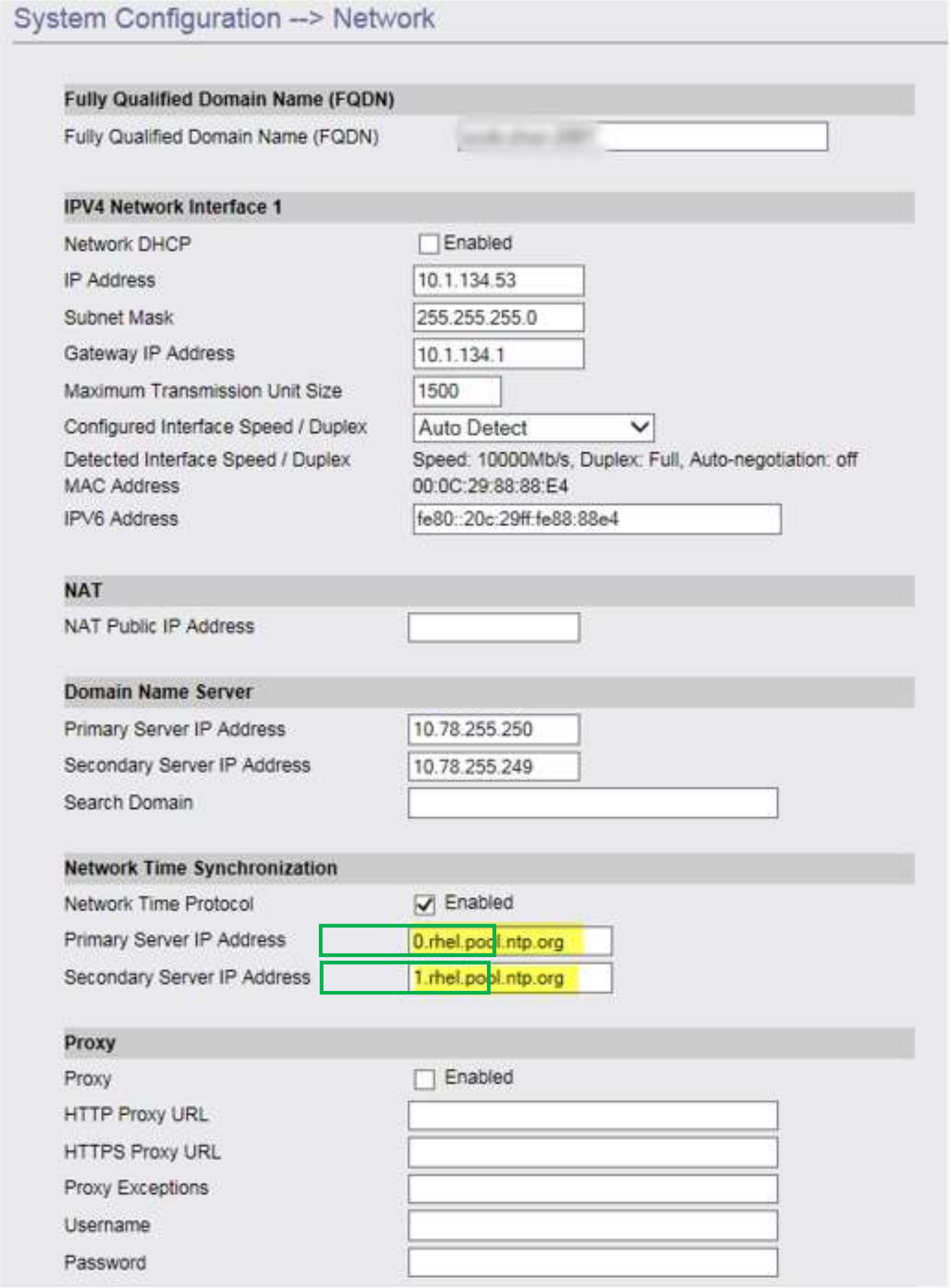
System Time

Date/Time (mm/dd/yyyy hh:mm): 9/11/2017 04:06

Time Zone: America/Chicago

Daylight Saving Time: ☑ Enabled

- System Configuration | Network and complete the following:
  - Enable NTP (Network Timing Protocol)
  - Configure the Primary and Secondary NTP Servers
    Note: NTP IP's to be confirmed by customer



System Configuration --> Network

Fully Qualified Domain Name (FQDN)

Fully Qualified Domain Name (FQDN)	[redacted]

IPV4 Network Interface 1

Network DHCP	□ Enabled
IP Address	10.1.134.53
Subnet Mask	255.255.255.0
Gateway IP Address	10.1.134.1
Maximum Transmission Unit Size	1500
Configured Interface Speed / Duplex	Auto Detect
Detected Interface Speed / Duplex	Speed: 10000Mb/s, Duplex: Full, Auto-negotiation: off
MAC Address	00:0C:29:88:88:E4
IPV6 Address	fe80::20c:29ff:fe88:88e4

NAT

NAT Public IP Address	

Domain Name Server

Primary Server IP Address	10.78.255.250
Secondary Server IP Address	10.78.255.249
Search Domain	

Network Time Synchronization

Network Time Protocol	☑ Enabled
Primary Server IP Address	0.rhel.pool.ntp.org
Secondary Server IP Address	1.rhel.pool.ntp.org

Proxy

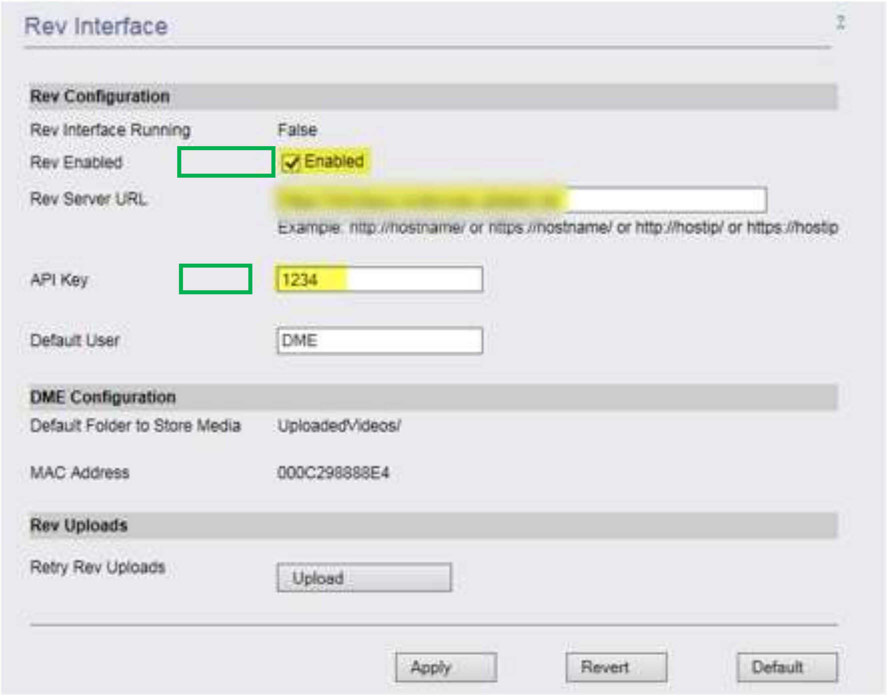
Proxy	□ Enabled
HTTP Proxy URL	
HTTPS Proxy URL	
Proxy Exceptions	
Username	
Password	

- Click the Apply button. The DME will reboot.

DME Integration to Rev

From VBrick DME Administrator Interface, navigate to:

- System Configuration | Rev Interface:
  - Set Rev Enabled to Enable
  - Add Rev Server URL
  - Add the API Key (supplied by REV portal administrator)



Rev Interface

Rev Configuration

Rev Interface Running False

Rev Enabled ☑ Enabled

Rev Server URL [redacted]

Example: http://hostname/ or https://hostname/ or http://hostip/ or https://hostip

API Key 1234

Default User DME

DME Configuration

Default Folder to Store Media UploadedVideos/

MAC Address 000C298888E4

Rev Uploads

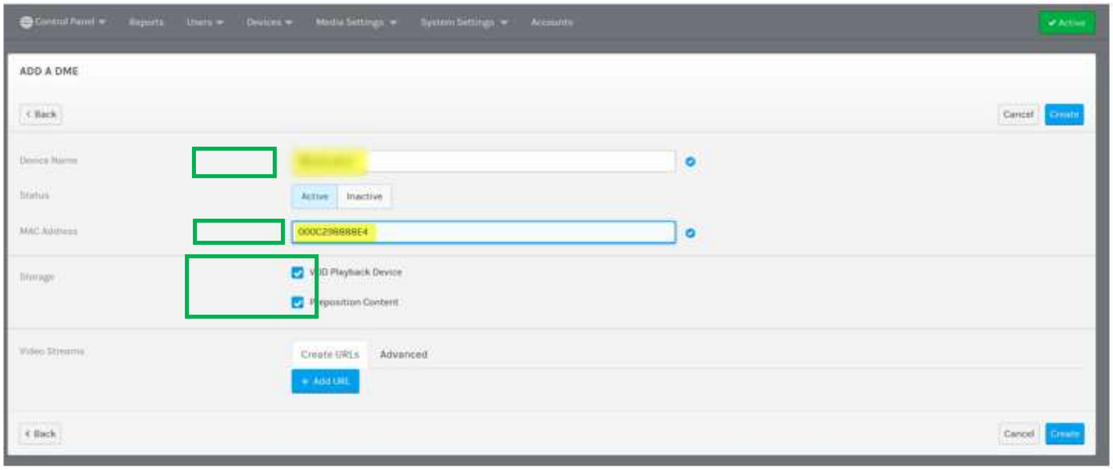
Retry Rev Uploads

- At the prompt, click OK to apply changes.

- On the VBrick REV portal, login with administrator access.
- Navigate to Admin | Devices | DME Management.
- Click on Add Device | Add DME button
  - Enter a Device Name for the DME
  - Enter the MAC address of the DME

  Under “Storage”, enable or disable, as needed the options for:

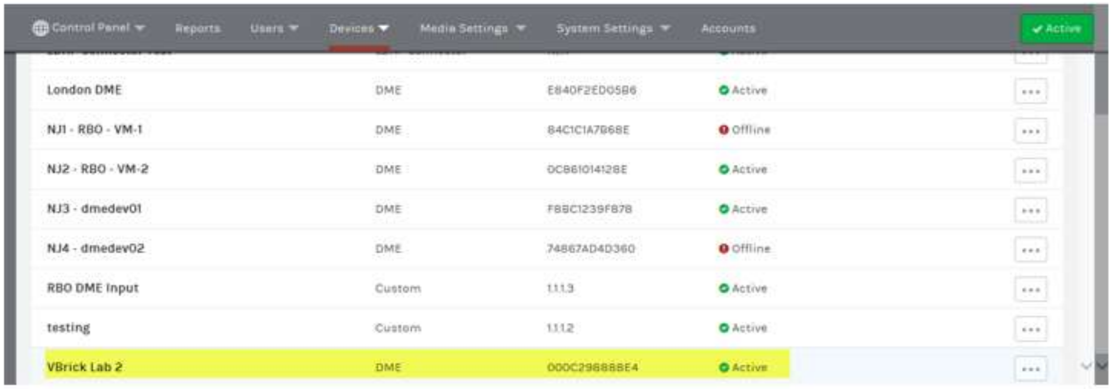
  - VOD Playback Device
  - Preposition Content



ADD A DME

Device Name	[illegible]
Status	Active / Inactive
MAC Address	000C298888E4
Storage	☑ VOD Playback Device ☑ Preposition Content
Video Streams	Create URLs / Advanced + Add URL

- Click the Create button.
  After a few seconds, the DME status should update from Uninitialized to Active:



London DME	DME	E840F2ED05B6	● Active
NJ1 - RBO - VM-1	DME	84C1C1A7B68E	● Offline
NJ2 - RBO - VM-2	DME	0C861014128E	● Active
NJ3 - dmedev01	DME	F8BC1239F878	● Active
NJ4 - dmedev02	DME	74867AD4D360	● Offline
RBO DME Input	Custom	1.1.1.3	● Active
testing	Custom	1.1.1.2	● Active
VBrick Lab 2	DME	000C298888E4	● Active

This completes initial actions for DME installation, configuration and REV integration.

Additional Best Practices

- Use FQDNs instead of “host names”
  - While using a “generic” host name may be OK in some circumstances, our experience shows that there are more and more situations where a FQDN (Fully Qualified Domain Name) is needed.
  - FQDNs are a pre-requisite for DMEs on which SSL certificates have to be deployed.

- SSL Cert for DMEs
  - A DME must be equipped with a SSL certificate, if:
    - Stream delivery must be done over https (as opposed to http)
    - That DME will be used as a ULS (User Location Services) agent, for Rev zoning
    - The DME accepts SSL certificates in PEM format.

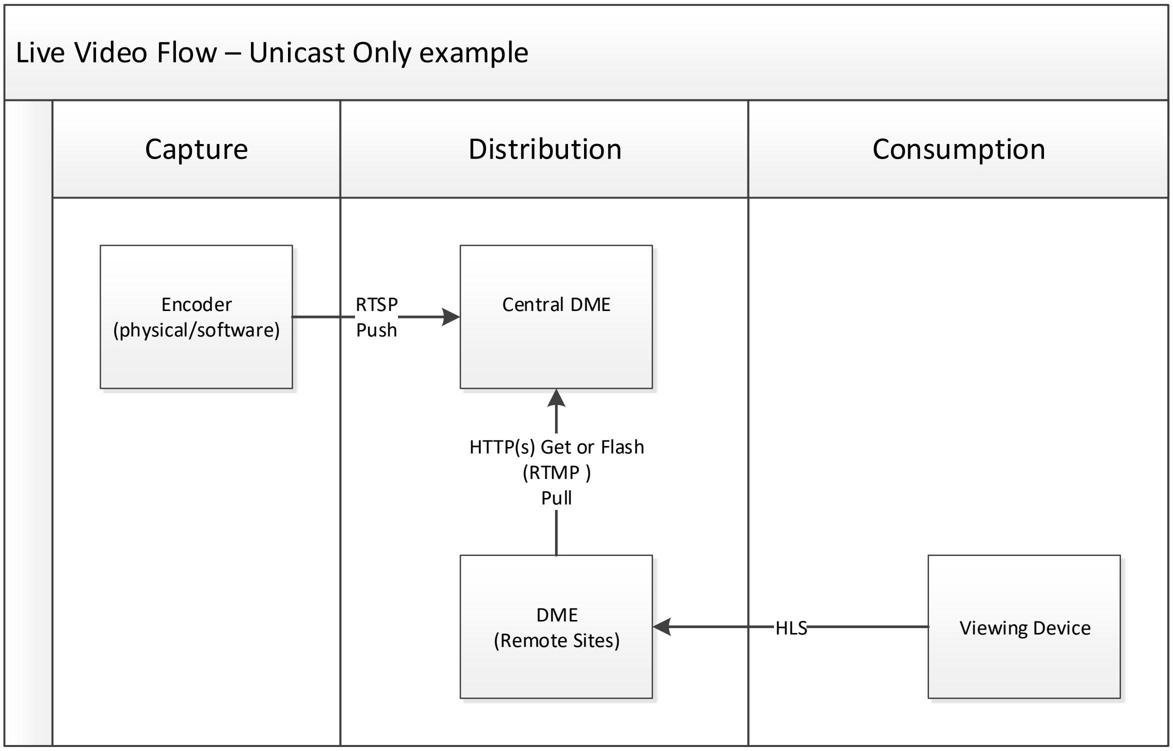
- QOS Tags
  - DMEs can be configured to insert DSCP QOS tags, as needed in the headers of certain streams (RTMP, RTSP, TS streams).
  - It is strongly recommended that the appropriate tag values are obtained in the early stages of the deployment.
  - It is best practice to configure the DSCP tags, in each DME, before building the stream distribution structure.
  - The DSCP tag can be configured in the DME UI, under **System Configuration** / **Streaming** / **Differentiated Services**.

- HLS Bandwidth Override - for MBR (Multiple Bit Rate) HLS playlists only, non Vbrick encoders
  - In order to properly serve MBR HLS playlists, the DME must have accurate bit-rate information available, for each playlist component.
  - The DME may have difficulties detecting the bitrate of certain non-Vbrick primary stream sources (Cisco TCS included). In such situations, the bit rate of each HLS stream should be entered manually, before that stream is enabled.
  - Configure this parameter in the DME UI, under **Output** / **HLS Steaming** / **Bandwidth Override** (must be set on each individual HLS stream).

Streaming and Distribution (On-premises or Cloud)

Overview

Steaming video includes 3 key components: capture, distribution, and playback as outlined below. The methods of stream distribution in the diagram indicate best practices.


Live Video Flow – Unicast Only example
Capture
Distribution
Consumption
Encoder (physical/software)
RTSP Push
Central DME
HTTP(s) Get or Flash (RTMP) Pull
DME (Remote Sites)
HLS
Viewing Device

The first segment is the "capture" section. We call this capture because this is where we being the encoding process. This involves configuring an encoder, TCS, or a streaming application to send to a DME. There are a number of methods to send the stream to the DME with RTSP Autounicast Push over UDP the preferred method for stream delivery. This is the method used when TCS is sending to the DME. With encoding applications such as Rev Create, the method is a RTMP (Flash) Push.

The next segment is Distribution. There are a number of possibilities and there are individual use cases that will dictate the method used. Where possible all DME's should be able to "see" each other via the ICP protocol and HTTP(s). If that is the case, the DME's caching capabilities, aka the "MESH," can be used for stream distribution. The advantage here is relatively little configuration to do. This is assuming an all unicast method of viewing.

Where ICP/HTTP(s) are blocked or multicast is required at the target DME's location, a manual method of fetching the stream must be performed. This will be accomplished via an RTMP (flash) Pull or RTMP Push. RMTP Push is preferred but the method used is based on any network rules.

The final segment is consumption which outlines how the stream will be viewed; whether by a user on a PC, by a user on a mobile device, or on a set top box.

VIEWING PROTOCOLS ---- HLS, RTMP, RTSP (FOR RECORDING)

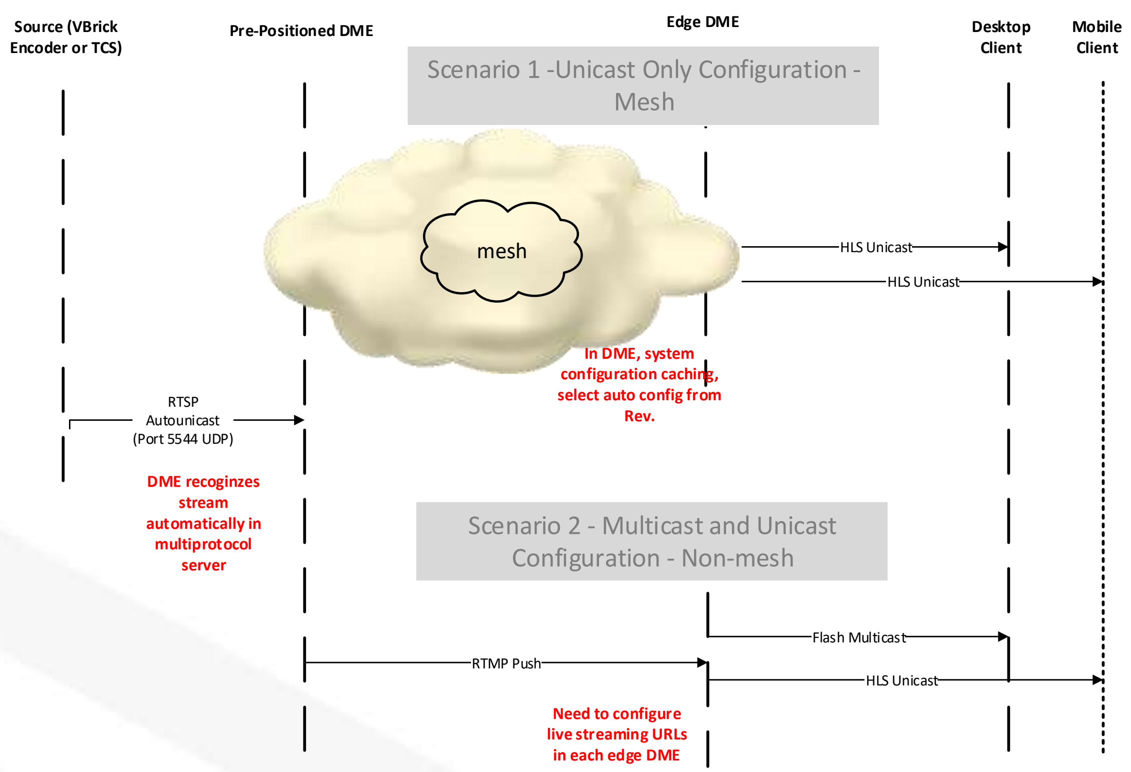
There are 2 primary viewing protocols for viewing a stream off of a DME. HTTP Live Streaming (HLS) is the primary method which is viewable on all Rev supported devices. The second is Flash multicast which isn't available for mobile devices.

RTSP is used for recording live webcasts. This requires no additional configuration.

Architecture and Design

LIVE STREAMING / DME TOPOLOGY

Live-Multicast/Unicast Streaming Configuration - Best Practice


Source (VBrick Encoder or TCS)
Pre-Positioned DME
Edge DME
Desktop Client
Mobile Client
Scenario 1 -Unicast Only Configuration - Mesh
mesh
HLS Unicast
HLS Unicast
RTSP Autounicast (Port 5544 UDP)
Scenario 2 - Multicast and Unicast Configuration - Non-mesh
Flash Multicast
RTMP Push
HLS Unicast

In DME, system configuration caching, select auto config from Rev.

DME recoginzes stream automatically in multiprotocol server

Need to configure live streaming URLs in each edge DME

Caveats
1, For both scenarios, will need to configure presentation profiles and zone logic in Rev.
2. HLS HTTP output streams must be configured on the DME.
3.
4.

VIEWING PROTOCOLS

There are 2 primary viewing protocols for viewing a stream off of a DME; HTTP Live Streaming (HLS) and Flash Multicast. For unicast viewing on any device, HLS is the preferred delivery method. The second method of using Flash multicast is only available for any browser only on desktop clients and is not available for playback on mobile devices.

RTSP unicast streams are only used for recording live webcast events in Rev. RTSP streams should only be added to Rev Presentation Profiles for the recordings. RTSP streams must not be added into any zone configurations.

IP NETWORK DELIVERY

The DME can deliver both multicast and unicast streams. The choice of each is dependent on the capabilities of the network. Where multicast has not been configured use unicast for stream consumption.

Multicast delivery is more bandwidth efficient and should be used if the streams are high bandwidth streams and/or the combination of user count and LAN capabilities would not support the bandwidth needed during a large event. Multicast configuration is inherently more complex and coordination will be required with the network team to ensure that it is fully tested before relying on it for the streaming of a live event.

The DME supports Quality of Service (QoS) with the tagging of packets originating from the multiprotocol server using a ToS bit. The DME uses Differentiated Services Code Point (DCSP) values to apply the QoS setting mainly to RTMP video (live and VOD). If tagging of VOD content is required, disable the HLS transcoding profile in Rev so that VOD has the appropriate QoS tag. In order for the DME to apply the QoS setting to each stream, each individual output stream must be disabled and then enabled.

AKAMAI

Overview

The Akamai RTMP publishing point provides the customer with an HTTP (HLS) stream, available for playback by off-network users. The source of the stream can be either the Vbrick 9000 Encoding Appliance or the Vbrick Distributed Media Engine (DME). The Vbrick devices are configured to transmit, or push, a RMTP stream configured with the setting provided by Vbrick, to the designated Akamai RTMP destination address. The viewing URL will be configured in the Rev portal as a “Custom Device” and added to the applicable Presentation Profiles and Zones.

Several new options for Akamai streaming have become available including an all HLS option where the DME is configured to transmit an HLS stream to an Akamai HLS publishing point. For more information, please contact the Vbrick Customer Success.

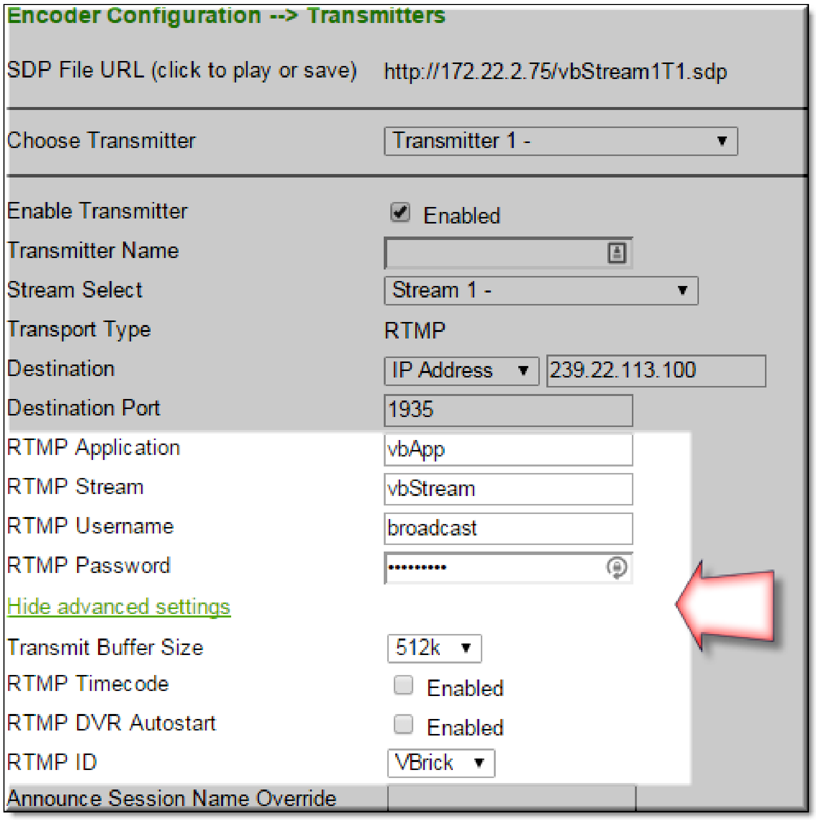
Ordering AKAMAI

Each Rev Cloud instance includes one Akamia Live streaming publishing point. The Akamai Publishing Popint is not automatically created at the time the Rev Cloud instance is created. In order for the Akamai Publihing Point to be created, an email must be sent to Vbrick Customer Support at support@vbrick.com. In the email please indication which type of Amakai Publishing Point you would like created, either Akamai Live HD (RTMP to HLS) or Akamai HLS (VC to HLS), and include the customer name and/or SalesForce Sale Order Number if available.

AKAMAI Topology

Vbrick has two devices that can be configured to transmit, push, a RTMP stream to an Akamai publishing point, the VB9000 encoder/presenter and the Distributed Media Engine (DME).

To configure the VB9000, a RTMP stream is configured and one of the encoder’s transmitters is configured to transmit the RTMP stream to the preconfigured Akamai RTMP Entry Point information provided by Vbrick.



Encoder Configuration --> Transmitters

SDP File URL (click to play or save)	http://172.22.2.75/vbStream1T1.sdp
Choose Transmitter	Transmitter 1 - ▾
Enable Transmitter	☑ Enabled
Transmitter Name	
Stream Select	Stream 1 - ▾
Transport Type	RTMP
Destination	IP Address ▾ 239.22.113.100
Destination Port	1935
RTMP Application	vbApp
RTMP Stream	vbStream
RTMP Username	broadcast
RTMP Password	•••••••••
Hide advanced settings	
Transmit Buffer Size	512k ▾
RTMP Timecode	□ Enabled
RTMP DVR Autostart	□ Enabled
RTMP ID	VBrick ▾
Announce Session Name Override	

-Destination IP Address:Port Number (Akamai FQDN Destination will be entered in the field)

-RTMP Stream Name

-RTMP Application

-RTMP Username

-RTMP Password

If using the Vbrick DME to transmit a RTMP to Akamai, configure a Flash Push in the DME’s Output Confguration page to the preconfigured Amakai RTMP Entry Point infrmiaton provised by Vbrick. The required information configured on the DME’s Flash Push page will be:

-Select the Stream Name in the drop down men selection

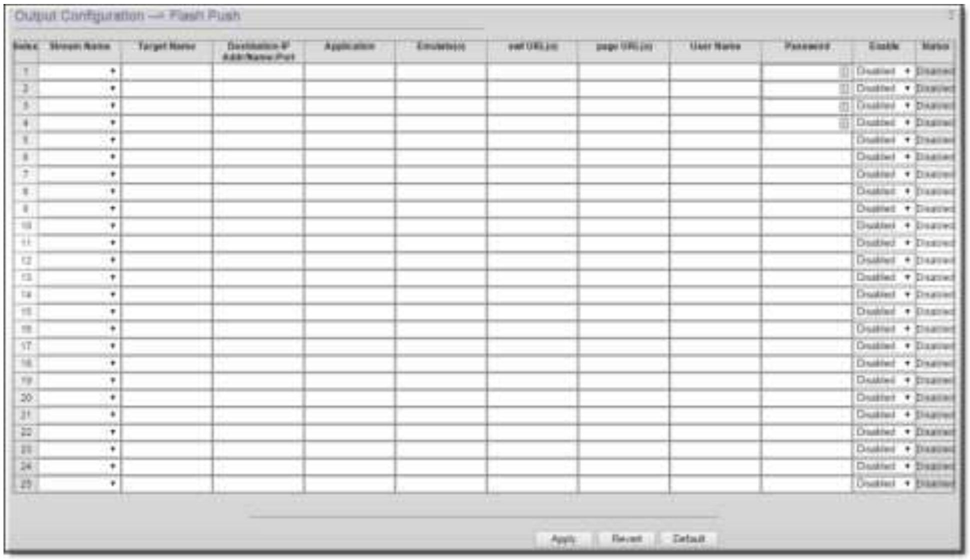
-Target Name (Stream Name)

-Destination IP Address:Port Number (Akamai FQDN Destination will be entered in the field)

-Application

-Username

-Password



Output Configuration — Flash Push

Index	Stream Name	Target Name	Destination IP Addr/Name:Port	Application	Emulate(s)	swf URL(s)	page URL(s)	User Name	Password	Enable	Status
1										Disabled	Disabled
2										Disabled	Disabled
3										Disabled	Disabled
4										Disabled	Disabled
5										Disabled	Disabled
6										Disabled	Disabled
7										Disabled	Disabled
8										Disabled	Disabled
9										Disabled	Disabled
10										Disabled	Disabled
11										Disabled	Disabled
12										Disabled	Disabled
13										Disabled	Disabled
14										Disabled	Disabled
15										Disabled	Disabled
16										Disabled	Disabled
17										Disabled	Disabled
18										Disabled	Disabled
19										Disabled	Disabled
20										Disabled	Disabled
21										Disabled	Disabled
22										Disabled	Disabled
23										Disabled	Disabled
24										Disabled	Disabled
25										Disabled	Disabled

If the customer network topology has an outbound firewall, the VB9000 or DME will need to be allowed to transmit the RTMP stream outbound to the internet to the Fully Qualified Domain Name (FQDN) of the Akamai Publishing Point on TCP Port 1935.

PUSH VS PULL

When determining to configure stream pushes, actively transmitting a stream from one DME with a destination to another DME, there are several factors to consider. First, if the network is segmented with fireawalls, configuring an Flash (RMTP) out to a remote DME may not require a firewall rule to be created in the firewall. Another consideration for configuring a push is if there are a small number of distributed streams from a primary DME out to remote DMEs.

In instances where a large number of streams are going to be configured and may reach the DME’s capacity for total number of output streams, configuring the destination, or remote, DMEs to pull a stream from the primary DME.

A pulled stream places the two DME's in a client-server type scenario with the client, pulling DME, connects to the primary DME (server) to request the stream.

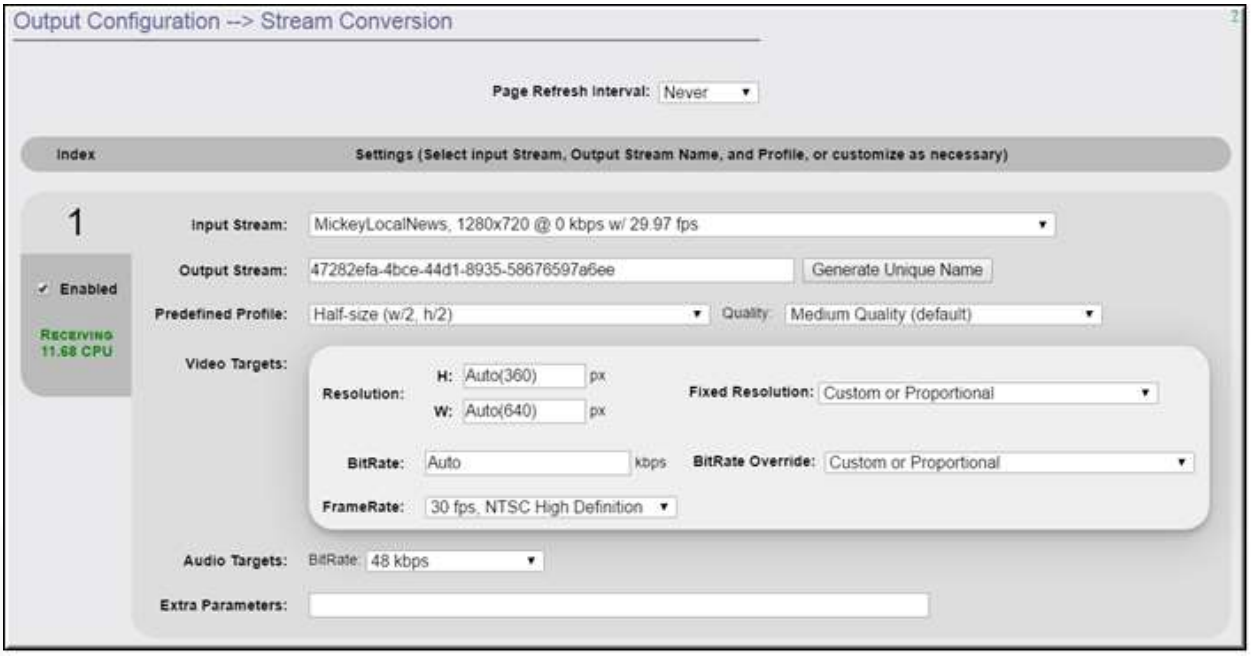
DME Model	Number of Configurable Input and Output Streams
7530	25
7550	35
7570	60

STREAM CONVERSION (TRANSRATING)

The **Stream Conversion** page provides a generalized transrating capability that allows modification of live streams in a number of ways. Here, you can transrate a stream to a lower bitrate, a different resolution, etc. The conversion process does not modify the resolution of the incoming stream, but creates a new stream that can used/viewed.

To help illustrate the use of this feature, here are a couple of use cases:

1. Locally creating an adaptive bitrate stream. Consider a remote DME that has limited bandwidth. It may be necessary to push/pull a single higher bitrate stream to that DME, and then transrate it to a number of reduced bitrate/resolution streams. Then, within the HLS Streaming page, they can be combined into a single stream for adaptive playback reflecting the unique needs of the remote viewers.
2. Create a Mobile sized Resolution and Bitrate stream. The DME can, if needed, take a stream and using this feature reduce the bitrate and resolution to be better provisioned to smaller form-factor mobile players.



Output Configuration --> Stream Conversion

Page Refresh Interval: Never

Index | Settings (Select input Stream, Output Stream Name, and Profile, or customize as necessary)

1

✓ Enabled

Receiving
11.68 CPU

Input Stream: MickeyLocalNews, 1280x720 @ 0 kbps w/ 29.97 fps

Output Stream: 47282efa-4bce-44d1-8935-58676597a6ee

Predefined Profile: Half-size (w/2, h/2)

Quality: Medium Quality (default)

Video Targets:

Resolution: H: Auto(360) px W: Auto(640) px

Fixed Resolution: Custom or Proportional

BitRate: Auto kbps

BitRate Override: Custom or Proportional

FrameRate: 30 fps, NTSC High Definition

Audio Targets: BitRate: 48 kbps

Extra Parameters:

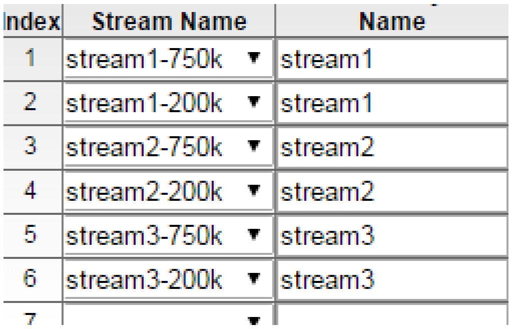
NOTE: This feature provides multiple levels of customization for stream size, resolution, and bitrate. However, software-based transrating features require a great deal of CPU resources depending on the complexity of the transrating configuration settings. For example, with Vbrick's internal benchmarks and using multiple, representative streams with the "HDTV 1080 – High Motion" predefined profile, it was found that, depending on the DME model, the CPU was impacted differently (e.g., on a DME 7530 there was 80-100% CPU utilization, while the 7550 saw 45-70% peaking to 90, and the 7570 a 6-9% utilization). This profile requires a great deal of processing. Looking at the opposite end, using the "Small Form Factor" profile, Vbrick observed a 10-30%, 6-10% and negligible utilization for DMEs 7530, 7550, and 7570 respectively. Please keep in mind that these impacts are additive based on the number of transrates the DME is performing. These examples are provided to illustrate the differences in CPU impacts and the necessity for end-user qualification and testing. Therefore, when using this feature please use a representative stream(s) (i.e, resolution, bitrate, framerate, motion) to

(1) test the quality of the transrated output,

(2) monitor the CPU usage to determine impact on the DME performance,

(3) perform multiple conversions to create a representative computational load mirroring how the DME will be used in production.

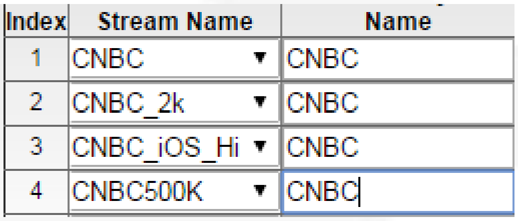
HLS is a progressive download streaming technology that creates a playlist containing segments of video packets to provide the end user with a quality viewing experience, while minimizing impact on network bandwidth. HLS streams may be configured with more than one stream combined into a master playlist. Combining the DME's Stream Conversion and HLS progressive download streaming capabilities is ideal for optimizing network bandwidth and providing the best quality stream to the end user no matter what type of device is used to view the stream.



Index	Stream Name	Name
1	stream1-750k ▼	stream1
2	stream1-200k ▼	stream1
3	stream2-750k ▼	stream2
4	stream2-200k ▼	stream2
5	stream3-750k ▼	stream3
6	stream3-200k ▼	stream3
7	▼	

The other way of building an HLS playlist is to use the DME's stream conversion feature where the DME will convert the stream into various bitrate settings based on predefined templates.

The three newly created streams are combined with the original, are configured into a HLS master playlist which gives even more variation in possible bandwidths when the stream is viewed on an end user's device.



Index	Stream Name	Name
1	CNBC ▼	CNBC
2	CNBC_2k ▼	CNBC
3	CNBC_iOS_Hi ▼	CNBC
4	CNBC500K ▼	CNBC

LIVE STREAMING DISTRIBUTION

Live Mesh

Design Considerations

- UC only or UC and MC
- WAN BW – from ABR perspective of whether to send 1 or 3 streams to remote DME
- WAN BW – from mesh perspective whereby edge DME needs both HLS and RTMP. HLS can be done via mesh or manually configured
- Control of Streams – if there is a desire to have a predefined hierarchy stream flow (regionalized deployment)

Redundancy

- No mechanism for active stream failover. Once a user is active on a stream and the stream goes down the user will have to refresh the browser to reconnect to a stream.
- Put 2 DMEs in one zone
- Front end 2 DMEs with a LB

Questions

- How does sister DME know what is closest DME to it to acquire content?

  Answer: If mesh used, the stream output is not viewable in the cached DME's multiprotocol server. To determin which stream the viewer is receiving, the user may use the browser's built in developer tools to identify which DME is providing the stream. This will make any troubleshooting efforts more difficult.

Manual Stream Configuration (when Live Mesh not used)

Manual stream configuration consists of configuring a stream from a video encoding appliance, such as the Vbrick 9000, and transmitting the stream from the encoding device into the DME's multiprotocol server (See DME Admin Guide). Once the incoming streams are received in the DME's multiprotocol server, the streams can be configured as RTMP or RTSP pushes to, or pulled RTMP or RTSP streams from, remote DMEs. The streams in the DME's multiprotocol server can also be transcoded into Flash Multicast and/or HLS streams for viewing in Rev.

To configure the streams for viewing in Rev as Live Event, there are two methods to creating the streams and assigning the live viewing URLs to the DME device. First, using the "Create Streams" function in the DME device management page (See Rev Admin guide), name the stream, select "create HLS URL", and then create to have Rev automatically create the HLS, RTSP, RTMP, and RTSP-TS streams in the DME and in Rev. If Flash Multicast will be used, these streams must be created manually on the DME and then added to the Advance Tab in the Video Sources section on the DME property page in Rev.

VOD MESH

VOD Mesh is configured automatically when Distributed Media Engines (DMEs) are added to to Rev and the option for VOD Playback is checked. Each DME configured with this setting will automatically added to neighboring DMEs for Mesh and caching of VOD content.

The other setting which determines if a DME will store a local copy of the VOD content or request a cached copy of the VOD file from a meshed DME is the “Prepositioned Content” option. If this option is checked, that DME will receive a local copy of the VOD content when the file is uploaded into Rev. Small DMEs deployed on a physical Cisco UCS server running VMware, are not enabled for prepositioned due to the limited amount of disk space available. The DME has a configuration setting located in the System Configuration/Streaming page to set the level of disk space reservered for caching VOD content.

LDAP and SAML (On-premises or Cloud)

SAML

OVERVIEW

SAML (Security Assertion Markup Language) is a single sign on mechanism that allows a trusted external "Identity Provider" to identify and authenticate a user for access to a "Service Provider" (in Vbrick's case: Rev). SAML is a secure method of validating a user's identity because it utilizes two different trust steps:

- Rev and the Identity Provider are set up by an administrator ahead of time to trust each other and exchange “Signing Keys” to verify messages are authentic messages.

When a user attempts to visit the “Service Provider” (Rev) then Rev redirects their browser to the “Identity Provider” login portal with a signed XML payload that verifies that the request is for access to an already trusted site (Rev). Once the “Identity Provider” has identified and authenticated a user it will redirect them back to the “Service Provider” (Rev) with a signed XML payload that includes the user’s username (and additional information if using SAML User Creation). Because the “Service Provider” (Rev) trusts the “Identity Provider” and can verify that the response is authentic (via the known Signing Key) then user will not be prompted for credentials by Rev.

CONFIGURATION

The majority of SAML configuration and maintenance is in the initial setup stage.

1) Ensure that Rev is configured to use HTTPS - most (though not all) "Identity Providers" will not accept "Service Providers" that only use

2) Download the "Service Provider Metadata" from the Rev Admin -> System Settings -> Security page. This XML document describes the key values that the "Identity Provider" will need to establish a trust relationship with Rev - the Signing Key "Signature" (a X.509 certificate), the entity ID, and the endpoint where responses will be sent. (Note, select the proper "Signature Algorithm" and "Sign SAML Request" option before downloading the metadata - changing these settings will invalidate the previously downloaded XML and you will need to re-download the metadata file)

3) Provide the downloaded vbrick.xml file to the administrator of the client's "Identity Provider" - common products are ADFS, Ping, OKTA and Trivoli. Some providers--notably ADFS--will accept the XML file directly for configuration. Others require you to enter in the information manually.
    - Entity ID: https://<rev.url>:443
    - SSO Endpoint: https://<rev.url>:443/sso/consume
    - Certificate: included in downloaded vbrick.xml, the contents of the <X509Certificate> node
    - Name Identifier: the value provided for name identifier (name ID) (OR the attribute specified in Rev settings) must match the Rev username of users. For example, using the default configuration of the LDAP Connector this value would be “sAMAccountName” for Active Directory.
4) Once the configuration is complete retrieve the “Identity Provider Metadata”, paste into the correct spot in the Rev Admin -> System Settings -> Security -> SSO section, enable SAML and save.
    - The Assertion should be signed but the Response should be unsigned
    - Both HTTP-POST and HTTP-REDIRECT endpoints should be included in IDP configuration
    - Setting up SAML – use LDAP, LDAP identifier used for username is what should get mapped to SAML identifier attribute used
    - Users already have to be imported into Rev before SSO can work.
    - SAML system needs to allow “SP Initiated” SSO bindings - Rev doesn't currently support IDP-initiated SSO
    - Once you turn on SSO new users don’t get user confirmation emails – Rev assumes they’ll login via SSO. So if you need to add a new local (non-SSO) user then you need to turn SSO back off first to get that user confirmation email/link.

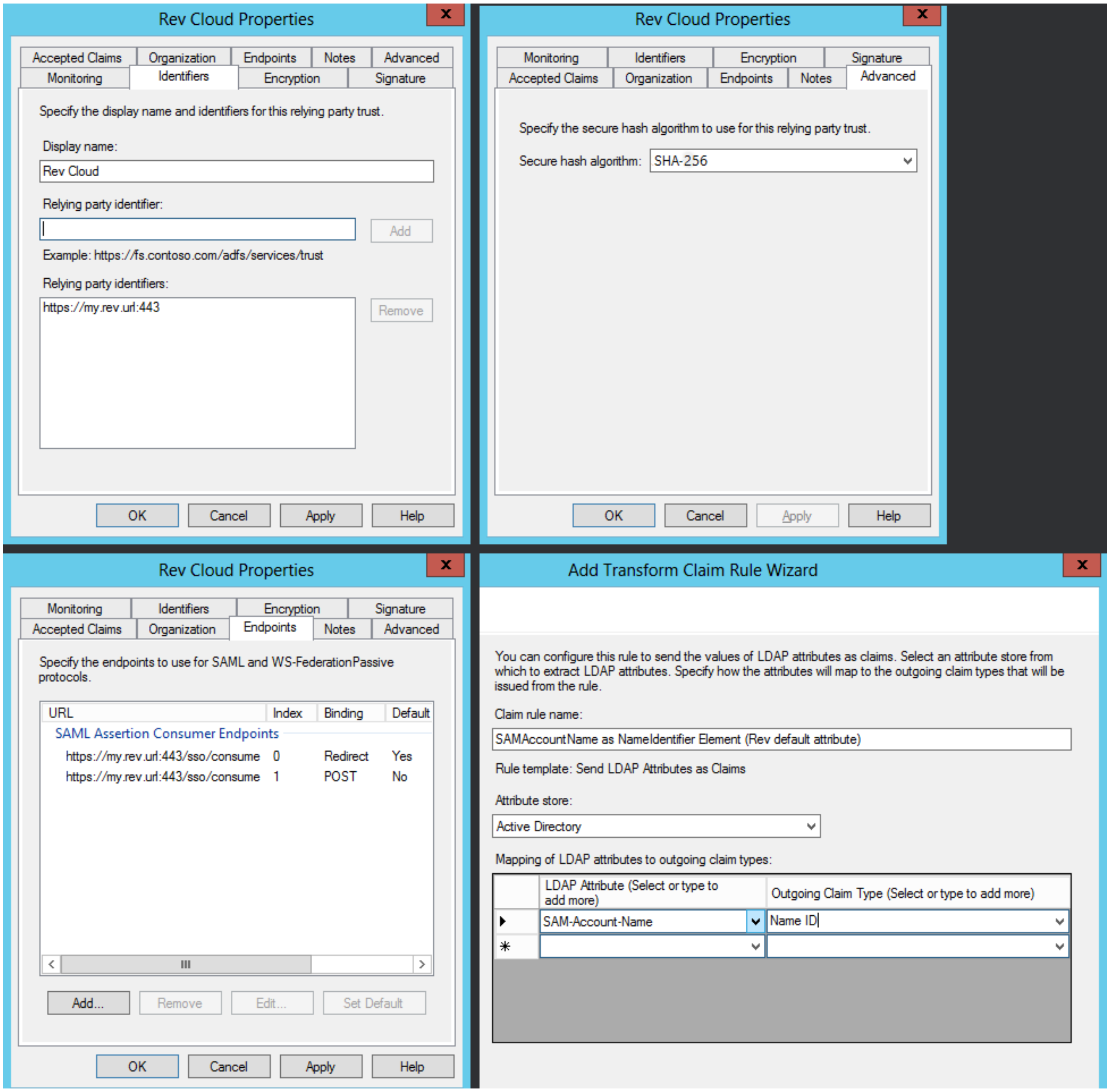
Configuring Rev SSO

REQUIREMENTS

Rev **MUST** be configured to use HTTPS before configuring SSO.

ADFS CONFIGURATION

1) Download the “Service Provider Metadata” from the Rev Admin page (see http://www.vbrick.com/help/rev/770/Admin%20Functions/SystemSettingsMenu.07.07.html#)
2) Within ADFS add a new Relying Party Trust based on the downloaded service provider metadata file (vbrick.xml)
3) Modify the resulting entry’s Properties and Claim Rules to match the below image (replacing “my.rev.url” with the URL of your Rev instance). Note that the LDAP Attribute set for the “Name ID” Outgoing Claim Type should match the “Username” attribute set in the LDAP Device configuration (the default is sAMAccountName).



Specify the display name and identifiers for this relying party trust.

Display name: Rev Cloud

Relying party identifier:

Example: https://fs.contoso.com/adfs/services/trust

Relying party identifiers: https://my.rev.url:443

Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm: SHA-256

Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default
SAML Assertion Consumer Endpoints			
https://my.rev.url:443/sso/consume	0	Redirect	Yes
https://my.rev.url:443/sso/consume	1	POST	No

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: SAMAccountName as NameIdentifier Element (Rev default attribute)

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
SAM-Account-Name	Name ID

4) Retrieve and save the ADFS Identity Provider Metadata (https://MY.ADFS.SERVER/FederationMetadata/2007-06/FederationMetadata.xml)
5) Copy the Identity Provider Metadata XML into the relevant field within the Rev Admin -> System Settings -> Security -> Single Sign On section.
6) If you matched the “Name ID” Outgoing Claim Type to the LDAP username attribute as directed in step 3 then select “NameIdentifier Element” for the “SAML Identity Location”. Otherwise, select “Attribute Element”, and enter the appropriate FULL attribute name (it’s a URL) as specified in the Identity Provider Metadata, which will look something like:

   <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="Name" xmlns="urn:oasis:names:tc:SAML:2.0:assertion"/>

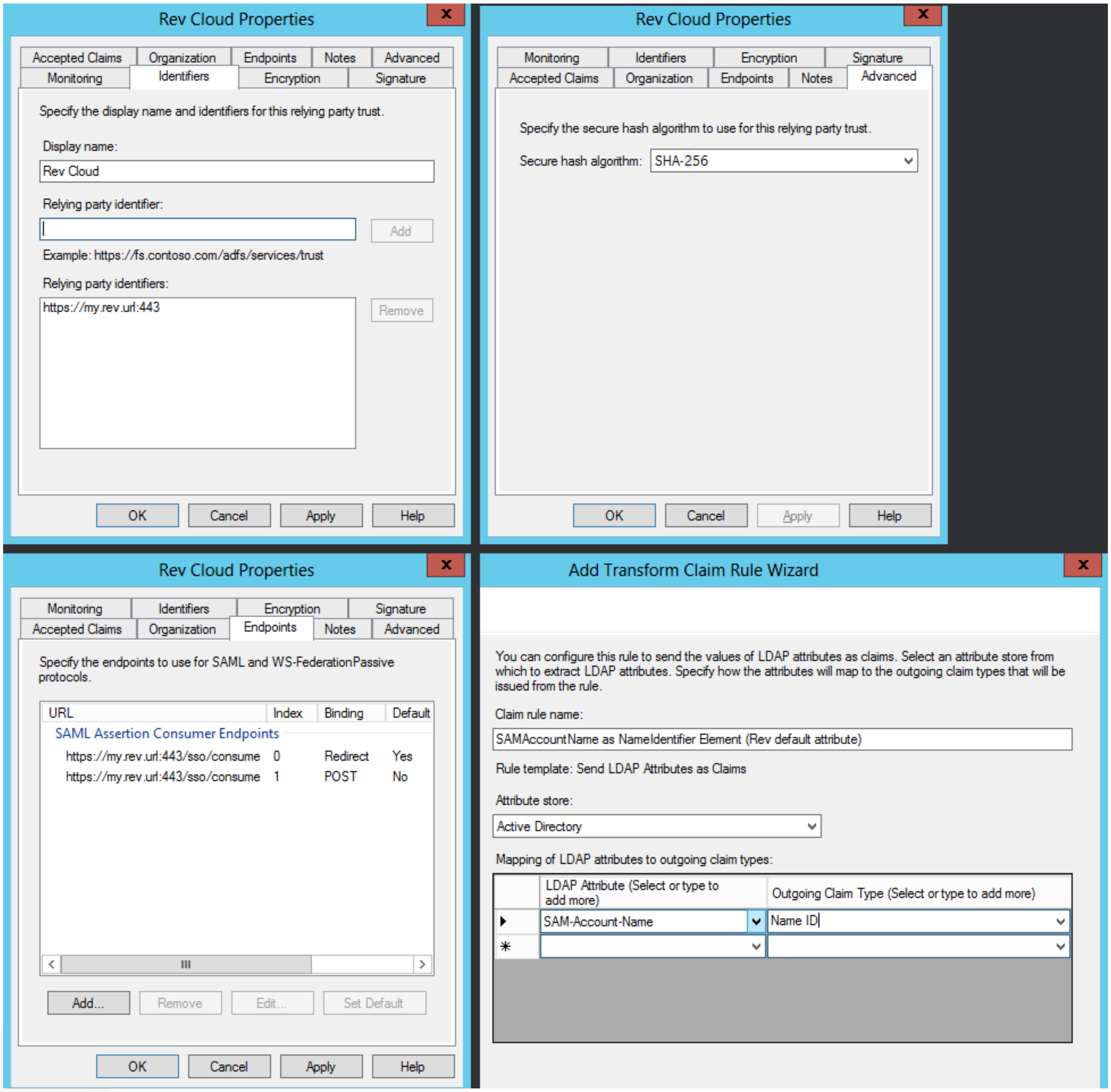
Check “Enable Single Sign On” to turn on SAML authentication, then click “Save” at the bottom of the page. Changes will immediately apply and when non-logged in users navigate to the main Rev URL the SSO login workflow will apply.

OKTA AND TIVOLI

Configure settings in a similar manner to the ADFS steps above, with the following caveats:

1) Match the Encryption hashing / signing algorithm to the Rev SSO Settings (SHA-1 or SHA-256)
2) **Rev does not support Identity Provider-initiated SAML**. If you include a link to Rev in your idp portal it should be a simple bookmark to https://my.rev.url , NOT an idp-initiated pointer to https://my.rev.url/sso/consume
3) **The Assertion should be signed but the response should be unsigned (don’t include ds:Signature in root of saml:Request)**
4) Ensure that you have a HTTP-Redirect binding enabled
5) Service Provider URL/identifier will be in the format https://my.rev.url:443/sso/consume, **NOT** https://my.rev.url/#/login . The port **must** be included in the URL

Here’s an example of an ADFS configuration for use with Rev



Rev Cloud Properties

Specify the display name and identifiers for this relying party trust.

Display name: Rev Cloud

Relying party identifier:

Example: https://fs.contoso.com/adfs/services/trust

Relying party identifiers: https://my.rev.url:443

Rev Cloud Properties

Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm: SHA-256

Rev Cloud Properties

Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default
SAML Assertion Consumer Endpoints			
https://my.rev.url:443/sso/consume	0	Redirect	Yes
https://my.rev.url:443/sso/consume	1	POST	No

Add Transform Claim Rule Wizard

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: SAMAccountName as NameIdentifier Element (Rev default attribute)

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
SAM-Account-Name	Name ID

Here’s an example of a known working configuration for OKTA

Single Sign On URL	https://my.rev.url:443/sso/consume
Recipient URL	https://my.rev.url:443/sso/consume
Destination URL	https://my.rev.url:443/sso/consume
Audience Restriction	https://my.rev.url:443
Default Relay State	
Name ID Format	Unspecified *(or any value)*
Response	Unsigned

Assertion Signature	Signed
Signature Algorithm	RSA_SHA1 *(or SHA256 – match Rev Settings)*
Digest Algorithm	SHA1 *(or SHA256 – match Rev Settings)*
Assertion Encryption	Unencrypted
SAML Single Logout	Disabled
authnContextClassRev	PasswordProtectedTransport
Honor Force Authentication	Yes
SAML Issuer ID	http://www.okta.com/${org.externalKey}

IMPORTANT NOTES

1) If you're unable to authenticate using SSO, the ADFS server is inaccessible or you're logging in using a local (non-LDAP) account then you may reach the regular login page by navigating to: http://my.rev.url/#/login , replacing "my.rev.url" with your Rev instance's URL.
2) Do not attempt to modify the contents of the "Service Provider Metadata" XML – the contents are signed, so any changes may cause authentication failures.
3) Rev's SAML implementation matches Users by their Username value. This username is matched to LDAP attributes which is set in the LDAP Device configuration (see http://www.vbrick.com/help/rev/770/index.html#page/Admin%2520Functions%2FAdminLDAP.10.2.html%23ww1145100)
4) Once Single-Sign On is enabled then manually-created users will not receive User Confirmation Emails. These links are available to Rev Users with the Admin role (see http://www.vbrick.com/help/rev/770/Admin%20Functions/UsersMenu.04.06.html).

Security (On-premises or Cloud)

Overview

This section provides a broad overview of Rev solution security requirements. If there are security elements relevant to specific areas, those are covered in that subsection of this document.

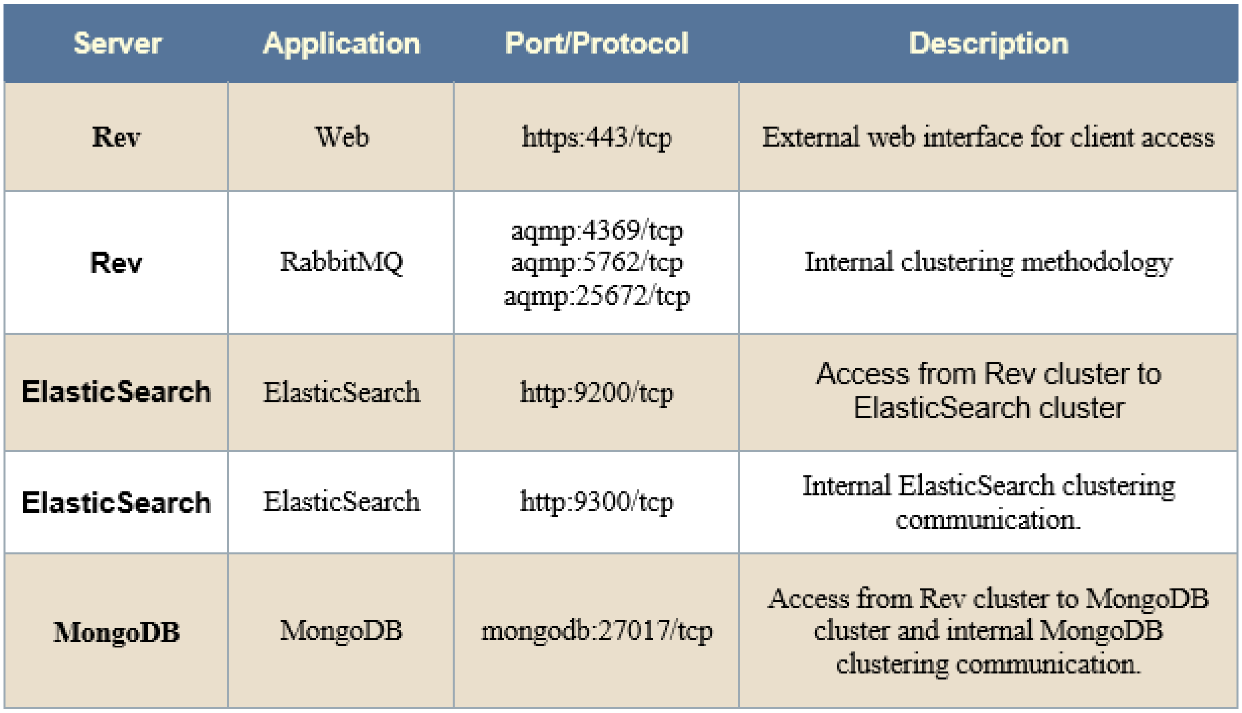
Ports and Firewalls

FIREWALL RULES

Below is a table of ports used between devices and the Rev portal, both for on premise Rev and Rev Cloud instances. Some of the devices and ports listed may not be used.

Source	Destination	Port/Protocol
Internal Users	Rev Load Balanced Internal IP	HTTPS
Internal Users	DME's	RTMP(1935)/TCP
		HTTP
		HTTPS
Vbrick Encoder	Core DME(s)	RTMP(1935)/TCP
		RTSP(5544)/TCP
		ICMP
	Rev Portal	HTTPS
All DME's	All DME's	RTMP(1935)/TCP
		RTSP(5544)/TCP
		MESH (3130)/UDP
		ICMP
TCS	Core DME(s)	FTP
		RTMP(1935)/TCP
		RTSP(5544)/TCP
		ICMP
External Users	Rev Load Balanced External IP	HTTPS
External Users	External DME(s) IP address	RTMP(1935)/TCP
		HTTP
LDAP Connector Server	Rev runtime (cloud)	HTTPS/443
LDAP	AD	LDAP 389
All DME's	Rev Load Balanced Internal IP	HTTPS

INTERNAL REV CLUSTER PORT CONNECTIONS FOR AN ON PREMISES REV IMPLEMENTATION



Server	Application	Port/Protocol	Description
Rev	Web	https:443/tcp	External web interface for client access
Rev	RabbitMQ	aqmp:4369/tcp aqmp:5762/tcp aqmp:25672/tcp	Internal clustering methodology
ElasticSearch	ElasticSearch	http:9200/tcp	Access from Rev cluster to ElasticSearch cluster
ElasticSearch	ElasticSearch	http:9300/tcp	Internal ElasticSearch clustering communication.
MongoDB	MongoDB	mongodb:27017/tcp	Access from Rev cluster to MongoDB cluster and internal MongoDB clustering communication.

ADDING SSL TO MONGO

If Mongo is using SSL, the VBrickPlatform.Runtime.Host.exe configuration file must be edited to set “usessl=true”, the “user=CN” field to the Subject of the Mongo Certificate, leave the password blank, and add the path to the Rev certificate in certificateFile and checkCertificateRevocation to false.

Example setting in the **VBrickPlatform.Runtime.Host.exe.config** file:

```
<mongo usessl="true" connectMode="Automatic" replicaSetName="" writeConcern="Acknowledged"
maxWaitQueueSize="10000" waitQueueTimeout="120" maxConnectionPoolSize="200" database="rev"
user="CN=*.vbrick-fips.com,OU=Rev,O=VBrick,L=Herndon,ST=VA,C=US" password="" retryCount="3"
delayMultiplierSeconds="1" certificateFile="c:/VBrick/Avenger/SSLCertificates/revuser.pfx"
checkCertificateRevocation="false">
  <servers>
    <server id="1" host="mongo1" port="27017" />
    <server id="2" host="mongo2" port="27017" />
  </servers>
</mongo>
```

Certificates

Certificates are required to be obtained and installed on one or more Distributed Media Engines (DME's) for a few system level configuration. One configuration where a certificate is required is in the use of the User Location Services for a Rev Cloud deployment. Rev will utilize the on premises DME to route clients based on their internal IP address into the correct Zone for viewing the live streams in Presentation Profiles and for viewing Video on Demand (VoD) files.

Another configuration requisite for installing certificates on the DME is for the use of the HTML5 player in the Rev portal. The certificate is required to be installed on the DME which will configure the DME to provide the HLS stream using HTTPS rather than the typical HTTP delivery method. The HTML5 player requires HTTPS delivery of HLS.

When using HTTPS access for an on prem Rev implementation, a SSL certificate must be installed on the HAproxy or other customer provided load balancer with the Rev portal URL as the FQDN. The HAProxy uses standard OpenSSL certificate commands for the generation of the Certificate Signing Request (CSR).

SSL certificates are not required to be installed on every on-prem server in the Vbrick Rev ecosystem, but can be installed and HTTPS configured on the servers at the request of the customer.

Event Planning and Support (On-premises or Cloud)

Overview

Please refer to the "Rev Event Runbook". This document provides a guide to executing webcast events.

Troubleshooting (On-premises or Cloud)

Common Issues

PROBLEM

User unable to login to Rev

TROUBLESHOOTING STEPS

1) Is user accessing the correct Rev URL?
2) Is user able to login to Rev using other browsers? Try IE, Chrome, and Firefox
3) Are other users able to login to Rev successfully?
4) Are user's proxy settings correct?
5) Is user a member of one or more AD groups imported into Rev?

PROBLEM

Video is slow to load

TROUBLESHOOTING STEPS

1) Are user's proxy settings correct?
2) Download the video-specific CSV report via the Rev UI. Verify the user is in the correct zone for their location and whether or not playback is being attempted from their local DME.

PROBLEM

Unable to find stored/live video in Rev (it is not listed)

TROUBLESHOOTING STEPS

1) Check permissions for the video and confirm that user has been granted access
2) Is the user able to see other content or do they see NO content?
3) Identify user's location
4) Check if the video completed the ingestion process? This is done by going to the "Advanced" tab of the video and confirming that there are one or more instances. If NO
   a. When video was uploaded, did user interface indicate a checkmark upon completion?
   b. When video was uploaded, did Rev display any errors? For example, an FTP error might be indicated here. If yes, what was the error displayed?
   c. Check if all DMEs are online

PROBLEM

Quality of video is poor

TROUBLESHOOTING STEPS

1) Check if player components are installed on client
   a. For flash, navigate to https://helpx.adobe.com/flash-player.html and click "Check Now"
2) Check if client firewall is configured to allow IGMP traffic.
3) Check that user's proxy settings are correct.
4) Run the video-specific CSV report. Verify that the user is in the correct zone and playing back from their local DME.

PROBLEM

All users are unable to see webcast slides

TROUBLESHOOTING STEPS

1) Check if Cloud slide delivery feature is enabled (see “Rev-Cloud Slide Delivery” section of this document). If enabled, check that required URLs are whitelisted.

SAML/SSO

- If logging in causes an infinite redirect (page keeps refreshing back to itself) then make sure the ADFS entry’s “Endpoints” include a HTTP-Redirect binding. This will appear in the Service Provider metadata as:
- <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://MY.ADFS. DOMAIN.COM/adfs/DOMAIN/"/>
- If you get an error message of “Invalid Relay State” they you’re probably attempting “Identity Provider Initiated SAML”. Rev only supports “Service Provider Initiated SAML” - the SAML negotiation workflow is initiated from Rev. Try navigating directly to http://my.rev.url , and confirm that SAML negotiation completes. Update your service portal to point directly to http://my.rev.url instead of using idp-initiated SAML.
- If login attempts redirect back to the Rev login page with an “invalid credentials” message:
  - **Make sure user exists in Rev with provided username and is not Suspended**
  - Check the Attribute Element Name set for the “SAML Identity Location” – ensure it matches an Attribute in the Identity Provider Metadata XML and that the specified attribute matches the LDAP Username setting.
  - Try copying the Identity Provider’s URL with query string (use the browser’s network capture tools to find the URL) and remove the XML signature portion from the end of the URL (highlighted in this example):
    - https://my.saml.idp.server.net/adfs/ls/?binding=urn%3aoasis%3anames%3atc%3aSAML%3a2.0%3abindings%3aHTTP-Redirect&SAMLRequest=...A REALLY LONG BASE64 ENCODED STRING...%3D%3D&RelayState=%2F&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&Signature=...ANOTHER BASE64 ENCODED STRING...

    If the Identity Provider throws an error *with* the xml signature, but proceeds *without* it then that may indicate that your ADFS server (or rarely Internet Explorer) has a Query String length limit. This may be avoided by choosing to turn off “Sign SAML Request” in the Rev SSO configuration.

- Rev On-Premise instances provide relevant SAML error information when logging is set to INFO in log4netConfig.xml.
  - Try searching for “SAML Request”, “SAML Response” and “Assertion” messages
  - If these logs include “XML Signature Validation” errors then ensure that the ADFS entry’s hashing algorithm matches the algorithm set in the Rev SSO setup (“SHA-1” or “SHA-256”).
  - “Assertion” messages should include the decoded Response XML. Note the <Attribute> values and ensure that the “Name” attribute matches what is included in the Rev Admin “SAML Identity Location” value (or the <NameID> XML Node exists when using the “Name Identifier” option).

- Tools
  - **Firefox Add-On**: SAML-Tracer: https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/
  - **Chrome Extension**: SAML Chrome Panel: https://chrome.google.com/webstore/detail/saml-chrome-panel/paijfdbeoenhembfhkhllainmocckace?hl=en
  - **IE**: Fiddler can be used to capture network traffic, including SAML requests.
  - **General**: This webpage includes a number of tools for decoding/debugging SAML: https://www.samltool.com

  - **General:** The Rev logs will contain helpful information, including decoded "SAML Request", "SAML Response" and "Assertion" messages when the logging level is set to "INFO".

- What to look for in decoded SAML requests/responses
  - A SAML Response will include a <samlp:StatusCode> XML node that indicates a successful or failed result from the ADFS/Identity Provider server. Generally this will show one of these values (for a full list see https://msdn.microsoft.com/en-us/library/hh269642.aspx):

<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />	The request succeeded, so failed requests occur in Rev's processing of the response. Check XML signing certificate (should only have one signing KeyDescriptor in IdP metadata and it should match the cert in the SAMLResponse) / encryption method (should be SHA-1), and ensure the "SAML Identity Location" is set to the correct Attribute Name.
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Responder" />	The request could not be performed due to an error on the part of ADFS/SAML Identity Provider. Check server configuration.

  - Make sure the Signature Method matches the Rev SSO configuration
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />