BMC REMEDY ITSM

AN EDGENEXUS ADC DEPLOYMENT GUIDE

Contents

Document Properties

Document Number: 2.0.7.1.21.09.07

Document Creation Date: June 30, 2021

Document Last Edited: July 1, 2021

Document Author: Jay Savoor

Document Last Edited by:

Document Referral: Choose an item. - **Version** Click or tap here to enter text.

Document Disclaimer

Screenshots and graphics in this manual may differ slightly from your product due to differences in your product release version. Edgenexus ensures that they make every reasonable effort to ensure that the information in this document is complete and accurate. However, Edgenexus assumes no liability for any errors. Edgenexus makes changes and corrections to the information in this document in future releases when the need arises.

Copyrights

Trademarks

Edgenexus Support

If you have any technical questions regarding this product, please raise a support ticket at: support@edgenexus.io

Introduction

This EdgeADC (ADC) application deployment guide is intended for persons administering the BMC Remedy ITSM and its load balancing. This document contains specific general suggestions and guidance, which may or may not be relevant for use within your organization.

BMC Remedy is one of the foremost IT service management applications used by thousands of organizations globally. In addition, BMC Remedy is used to receive and service IT support requests by its employees.

We recommend the following:

The ADC is deployed as a pair of appliances in either a virtualization technology, installing it as a virtualized appliance or as a hardware appliance in approved server hardware.

When external users access the network via the Internet, we recommend that the ADC pair is deployed in the DMZ and the traffic rerouted through the firewall to the LAN zone.

The ADC's operate in a high-availability (HA) mode when placed in pairs and provide you the level of redundancy and resilience required for mission-critical systems.

The ADC is fully capable of load-balancing your BMC Remedy ITSM, and this guide explains how to set this up.

Prerequisites for supporting BMC Remedy ITSM

As usual, it is assumed that the person who is installing and configuring the ADC is familiar with the terminology used within this document and networking in general. We strongly suggest that both the network technician and BMC Remedy ITSM administrator work in tandem when setting up the load balancing and that this is first done for a sandbox environment before replicating to the production environment.

Further, it is also recommended you follow the below requirements, which are regarded as the minimum:

- The latest ADC firmware should be used
- The BMC Remedy ITSM software should be installed and operational.
- The initial ADC configuration should be done against the BMC Remedy ITSM sandbox deployment.
- DNS entries for both internal and external access should be configured and working.
- The ADC should be reachable using a web browser and the management IP.

Acronyms used

VIP – Virtual IP	VS – Virtual Service
RS – Real Server	RSIP – Real Server IP
ADC – Edgenexus EdgeADC	

VIPs, Ports, and Other Bits

Several modules go to make up the BMC Remedy system, some of which can be load-balanced while others cannot, depending on how the containing environment has been designed. The BMC Remedy AR and the Mid Tier modules can be load balanced using the ADC, either singly or as a complete solution.

When load balancing BMC Remedy ITSM, the following VIPs will be needed for operations.

BMC AR API Service

- This VIP forms the load-balanced communication channel for the AR API accesses.

Port	Protocol	Service Type	Explanation
7654	TCP	L4-TCP	BMC Ready AR Server API

HTTP/HTTPS Remedy Mid Tier Service

- This VIP/VS handles client access communications to the Mid Tier servers.

Port	Protocol	Service Type	Explanation
8080	TCP	L4-TCP or L7 HTTP	This port is used to handle all HTTP requests from clients. You can use Layer 4 TCP with SSL Passthrough or Layer 7 with SSL Bridging.
8443	TCP	L4-TCP or L7 HTTPS	This port is used to handle all HTTPS requests from clients. You can use Layer 4 TCP with SSL Passthrough or Layer 7 with SSL Bridging.

Sizing the EdgeADC

The ADC can operate in either physical or virtual deployments. The reverse proxy engine within the ADC is optimized for speed and efficiency. The ADC will use all available threads automatically.

In virtualized environments, we recommend that you set the ADC to 4 vCPU with 8GB RAM, to begin with, and scale up when you need to.

We recommend that you utilize the hardware platforms from our partners in physical environments, with the base system being a quad-core Intel Xeon with 8GB RAM.

In both cases, 50GB of disk storage space should be sufficient.

Deployment Scenarios

Connections to the BMC Remedy ITSM system occur by connecting to the VIP or Virtual IP service created on the ADC. The ADC then load-balances the connections to the nodes configured within the ADC and linked to the VIP. An example diagram is shown below.
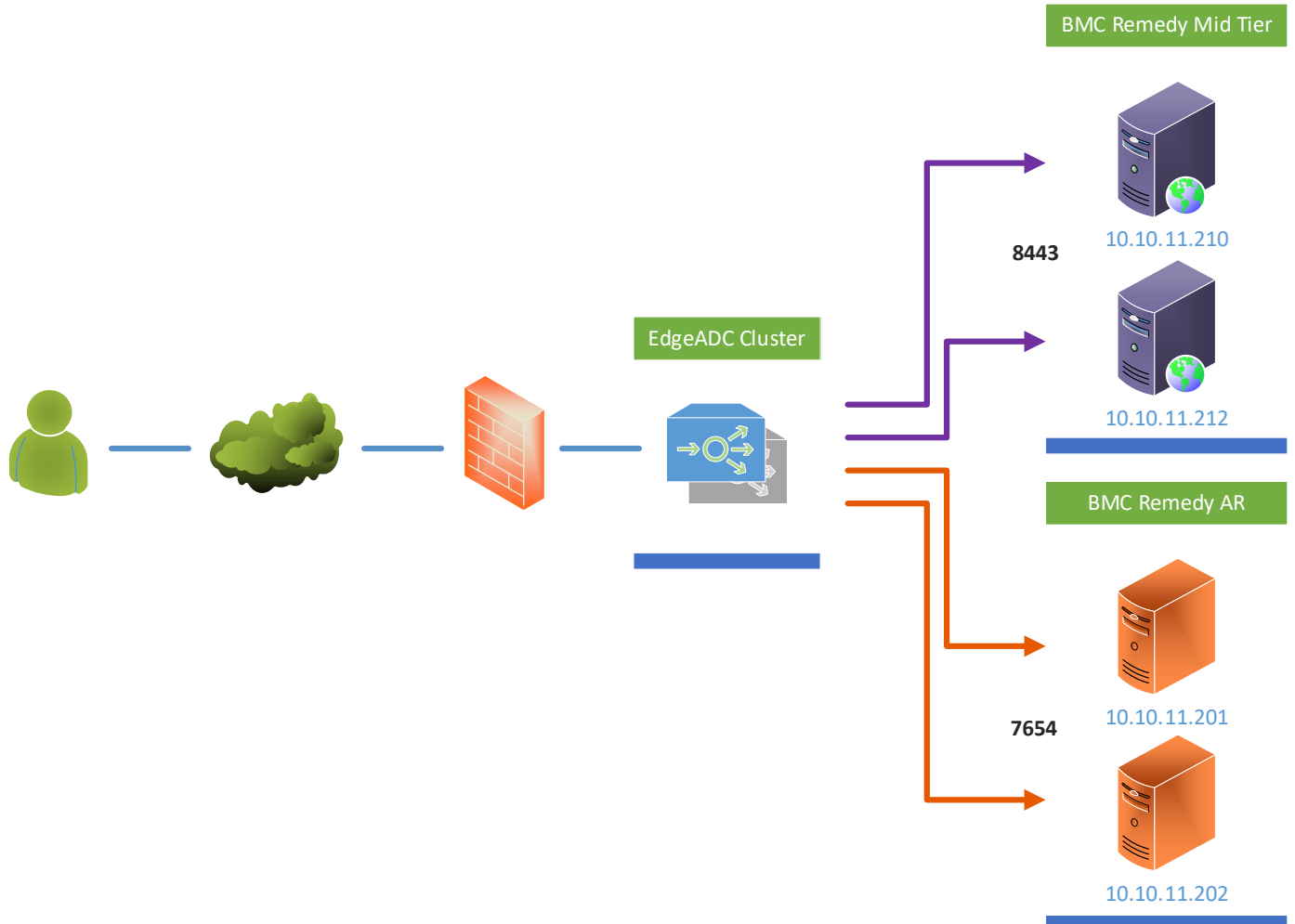
Virtual Service Methods

There are several methods of configuring the ADC for use with BMC Remedy ITSM.

SSL Passthrough   In this mode, the traffic enters the ADC on port 443 using SSL. Then, the traffic is sent onto the nodes without inspection. ADC service type Layer 4 TCP is used.

SSL Bridging   In this mode, the SSL traffic is terminated in the ADC and then re-encrypted before passing to the nodes. When this mode is chosen, you will need to have the SSL certificate installed on the nodes and install it in the ADC. This mode is the recommended best practice method for security reasons. ADC service type HTTP is used.

The following pages will take you through the VIP configuration. Please take care to configure correctly to avoid issues in operations.

Clustering the EdgeADC

The EdgeADC can operate as a stand-alone appliance, and it is incredibly reliable. However, in terms of best practice, we must accept that it is as critical as the servers it is load balancing, and we would therefore recommend placing it in a cluster.

- First, stand up a second EdgeADC in the same subnet as the primary.
- Once you have licensed it logon to your Primary EdgeADC
- Proceed to System > Clustering
- You should see the page as below.

- You will notice that there are two panels within the Management panel. On the left is the Unclaimed panel. On the right is the Cluster showing the cluster members, their priority, and status.
- In between the two panels is a cluster of arrow buttons.
- Click on the EdgeADC that is in the Unclaimed Panel and click the RIGHT arrow button.
- This action moved the unclaimed EdgeADC into the cluster.
- Immediately it is moved across; the Primary will replicate its settings, including VIPs to the secondary. Note that any apps you have added to the Primary will not be replicated to the Secondary – examples are WAF, GSLB, etc.
- After clustering, the Management panel should look like the one below.

BMC Remedy AR VIP – Using Layer 4

The method being used here is SSL Bridging. In this method, the SSL traffic enters the ADC, is then terminated internally, any inspection required is carried out, and the traffic is then re-encrypted and sent to the nodes.

- The first step is to create the VIP and initial VS
- Log into the ADC and go to IP Services. This location should be the default entry point.
- Click Add Service
- You will see an empty row into which you will add values similar to the one below. The field values we provide are examples for your reference.

IP Address	Subnet Mask	Port	Service Name	Service Type
10.10.10.222	255.255.255.0	7654	*REMEDY AR*	Layer 4 TCP

So this has now created the initial VIP with the entry IP address of 10.10.10.222. In this example, we show a NAT IP address, and the assumption is that there is a firewall between the ADC and the public Internet. You can, of course, have a public IP address as the VIP entry point.

- Now we will define the Real Servers (RS) section.
- Click on the Servers tab to display the Real Servers listing.
- There is a ready-created blank entry to aid you in adding the RS entries.
- Please enter the details relevant to your infrastructure following the examples we have provided below. In our case, we have three array nodes, but you may have more.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.11.201	7654	100	100	AR Node 1	1

- Click Update to save.
- Click the Copy Server button and make changes for the second array node.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.11.202	7654	100	100	AR Node 2	2

- Click Update to save.

You can add a name for the server group if you wish.

The next stage is to configure the Basic tab.

- Click on the Basic tab within the Real Servers section.
- Make changes as follows:

Field	Value
Load Balancing Policy	Least Connections
Server Monitoring	TCP Connect
Caching Strategy	Off
Acceleration	Compression
Virtual Service SSL Cert	None
Real Server SSL Cert	None

- Click Update when done.

There are no configurations to be done within the Advanced tab.

BMC Remedy Mid-Tier VIP – Using Layer 7

The method being used here is SSL Bridging. In this method, the SSL traffic enters the ADC, is then terminated internally, any inspection required is carried out, and the traffic is then re-encrypted and sent to the nodes.

- The first step is to create the VIP and initial VS
- Log into the ADC and go to IP Services. This location should be the default entry point.
- Click Add Service
- You will see an empty row into which you will add values similar to the one below. The field values we provide are examples for your reference.

IP Address	Subnet Mask	Port	Service Name	Service Type
10.10.10.224	255.255.255.0	8443	*REMEDY AR*	HTTP

- Now we will define the Real Servers (RS) section.
- Click on the Servers tab to display the Real Servers listing.
- There is a ready-created blank entry to aid you in adding the RS entries.
- Please enter the details relevant to your infrastructure following the examples we have provided below. In our case, we have three array nodes, but you may have more.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.11.210	8443	100	100	Mid-Tier Node 1	1

- Click Update to save.
- Click the Copy Server button and make changes for the second array node.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.11.212	8443	100	100	Mid-Tier Node 2	2

- Click Update to save.

You can add a name for the server group if you wish.

The next stage is to configure the Basic tab.

- Click on the Basic tab within the Real Servers section.
- Make changes as follows:

Field	Value
Load Balancing Policy	Least Connections
Server Monitoring	TCP Connect
Caching Strategy	Off
Acceleration	Compression
Virtual Service SSL Cert	Your SSL PFX Certificate
Real Server SSL Cert	Any

- Click Update when done.

There are no configurations to be done within the Advanced tab.

Note: To add your SSL certificate, please consult the EdgeADC Administration Guide

BMC Remedy Mid-Tier VIP – Using Layer 4

The method being used here is SSL Passthrough. In this method, the SSL traffic enters the ADC, and the traffic is then immediately sent to the nodes without any SSL re-encryption.

- The first step is to create the VIP and initial VS
- Log into the ADC and go to IP Services. This location should be the default entry point.
- Click Add Service
- You will see an empty row into which you will add values similar to the one below. The field values we provide are examples for your reference.

IP Address	Subnet Mask	Port	Service Name	Service Type
10.10.10.224	255.255.255.0	8080	*REMEDY AR*	Layer 4 TCP

- Now we will define the Real Servers (RS) section.
- Click on the Servers tab to display the Real Servers listing.
- There is a ready-created blank entry to aid you in adding the RS entries.
- Please enter the details relevant to your infrastructure following the examples we have provided below. In our case, we have three array nodes, but you may have more.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.11.210	8080	100	100	Mid-Tier Node 1	1

- Click Update to save.
- Click the Copy Server button and make changes for the second array node.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.11.212	8080	100	100	Mid-Tier Node 2	2

- Click Update to save.

You can add a name for the server group if you wish.

The next stage is to configure the Basic tab.

- Click on the Basic tab within the Real Servers section.
- Make changes as follows:

Field	Value
Load Balancing Policy	Least Connections
Server Monitoring	TCP Connect
Caching Strategy	Off
Acceleration	Compression
Virtual Service SSL Cert	None
Real Server SSL Cert	None

- Click Update when done.

There are no configurations to be done within the Advanced tab.

The Finished Solution

BMC Remedy AR VIP

BMC Ready Mid Tier VIP

BMC Remedy Real Server Basic Tab