DEPLOYMENT GUIDE

Ruckus SmartZone Cluster Redundancy Deployment Guide

This deployment guide is based on SmartZone 5.1 GA and later.

Part Number: 800-72143-001 Rev A
Publication Date: 14 February 2019

Copyright, Trademark and Proprietary Rights Information

© 2019 ARRIS Enterprises LLC. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from ARRIS International plc and/or its affiliates ("ARRIS"). ARRIS reserves the right to revise or change this content from time to time without obligation on the part of ARRIS to provide notification of such revision or change.

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, ARRIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. ARRIS does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. ARRIS does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to ARRIS that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL ARRIS, ARRIS AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF ARRIS HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface

Purpose of This Document

The purpose of this deployment guide is to provide an understanding of SmartZone Cluster Redundancy and the deployment options for your network. This guide describes the following deployment options:

- Active-Standby Virtual SmartZone with a single virtual data plane
- Active-Standby Virtual SmartZone with multiple virtual data planes
- Active-Active Virtual SmartZone with a single virtual data plane
- Active-Active Virtual SmartZone with multiple virtual data planes
- Active-Standby SmartZone 300
- Active-Active SmartZone 300

Audience

This document can be used by system engineers and customers to gain an understanding of SmartZone Cluster Redundancy.

Objectives

The objective of this guide is to assist the engineers in understanding SmartZone Cluster Redundancy deployment.

This deployment guide covers the following topics:

- How the SSH tunnel and Ruckus GRE tunnel fail over in cluster redundancy
- How to deploy the Ruckus controller and data plane (or virtual data plane) with cluster redundancy
- The difference between Active-Active and Active-Standby cluster redundancy
- Caveats and limitations of cluster redundancy

Document History

Date	Part Number	Description
February 14, 2019	800-72143-001 Rev A	Initial release.

Overview

Cluster redundancy benefits your Wi-Fi deployment in a number of ways:

- In Active-Active cluster redundancy, different controllers at different data centers, or different regions, can back up each other.
- Access points (APs) and virtual data planes (if the deployment uses Virtual SmartZone and the virtual data plane) have a backup controller when their primary data center is down.
- All the controllers in Active-Active cluster redundancy provide service at the same time.
- In Active-Standby cluster redundancy, multiple controllers (or clusters) can share the same backup controllers (or clusters) one at a time.

Active-Active and Active-Standby cluster redundancy (including a virtual data plane) are designed for:

- The following cases where users cannot have all the controllers in the same cluster:
  - Bandwidth limitations on the cluster link.
  - A SZ300 or vSZ-H with three NIC controllers has a cluster interface on a different network and cannot use a Layer 2 link.
  - A different controller needs to manage different regions separately.
  - Having a backup controller (or cluster) from different controllers (or clusters).
  - Multiple one-node clusters to back up each other.
- SmartZone 5.1 GA and later (SmartZone 3.6 or 5.0 does not support the virtual data plane and Active-Active cluster redundancy).
- Virtual SmartZone model H (vSZ-H) and SZ300.
- Controllers are on different clusters at different locations.
- Either Active-Active or Active-Standby cluster redundancy.

NOTE
Cluster redundancy is different than a cluster where all the controllers in the same cluster share the same database.

Is Cluster Redundancy the Right Solution for Your SmartZone Deployment?

There are two different options for SmartZone Cluster Redundancy: Active-Active and Active-Standby.

Active-Active Cluster Redundancy

Active-Active cluster redundancy may be the right option for addressing the following deployment scenarios:

- The required latency for SmartZone cluster traffic is lower than the latency between the controllers (also called nodes in a Ruckus cluster) in the current deployment.
- Requires a backup controller for the access point and virtual data plane (if deployment is using Virtual SmartZone) to fail over when the current controller is down.
- The backup controller is also an active controller that provides the service for other Wi-Fi deployments.

Active-Standby Cluster Redundancy

Active-Standby cluster redundancy may be the right option for addressing the following deployment concerns:

- The required latency for SmartZone cluster traffic is lower than the latency between the controllers (also called nodes in a Ruckus cluster) in the current deployment.
- Budget limitations on the controller license.
- Requires a backup controller for the access point and virtual data plane (if deployment is using Virtual SmartZone) to fail over when the primary controller is down.

How the SSH Tunnel and Ruckus GRE Tunnel Fail Over in Cluster Redundancy

Tunneling in Ruckus Devices

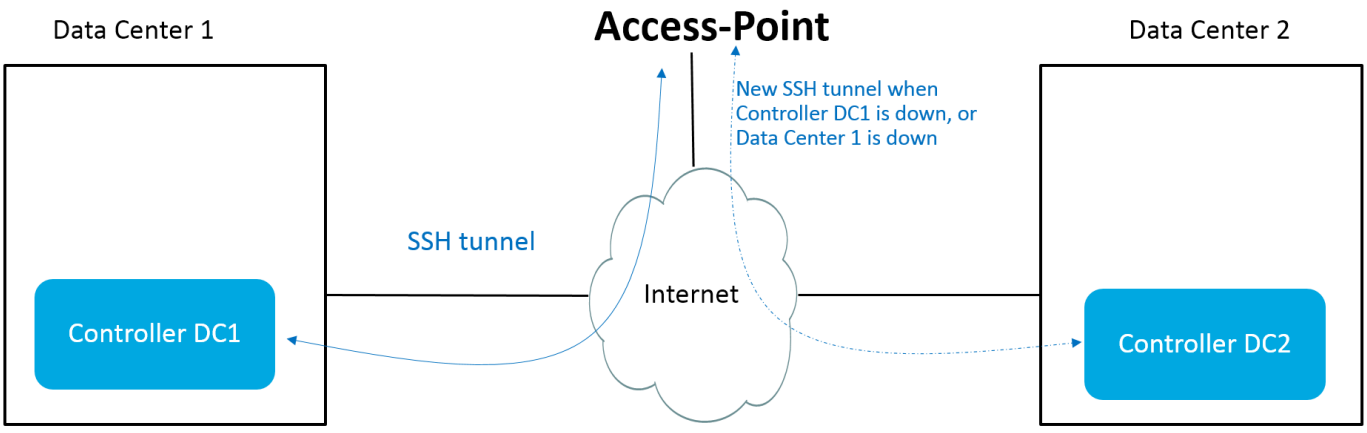
- The SSH tunnel is established between:
  - Access point (AP) and controller (SmartZone and Virtual SmartZone).
  - Virtual data plane and virtual controller.
- The Ruckus GRE proprietary tunnel is established between an access point (AP) and the virtual data plane or SmartZone data plane.

NOTE
To ensure the AP and virtual data plane receive the same configuration when moving to the new controller (or cluster), a configuration synchronization is scheduled to synchronize the configuration from a selected primary controller (or cluster) to another controller (or cluster). This configuration synchronization traffic is sent by way of the management (MGMT) interface of the controllers.

AP SSH Tunnel Failover Between Different Controllers (or Clusters)

The AP SSH tunnel is established between the control interface of the controller and the access point. When the AP does not receive the heartbeat response from the controller, the AP switches to an IP address in the failover list, and registers to the new controller (or cluster).

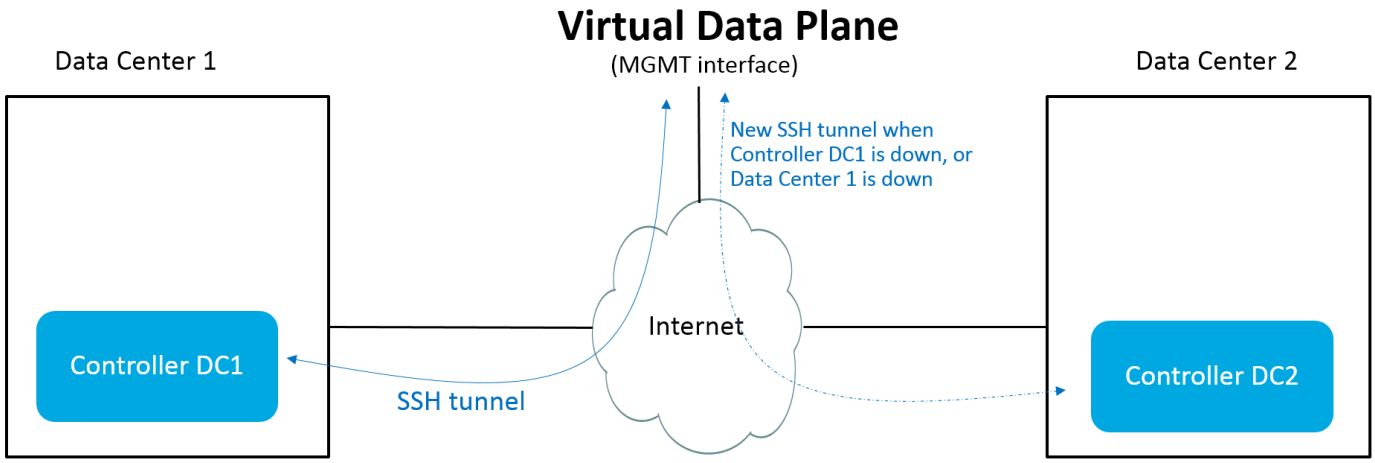
FIGURE 1 AP SSH Tunnel Failover Between Different Controllers (or Clusters)



Virtual Data Plane SSH Tunnel Failover Between Different Controllers (or Clusters)

The virtual data plane SSH tunnel is between the control interface of the controller and the management (MGMT) interface of the virtual data plane. When the virtual data plane does not receive the heartbeat response from the controller, the virtual data plane switches to an IP address in the failover list, and registers to the new controller (or cluster).

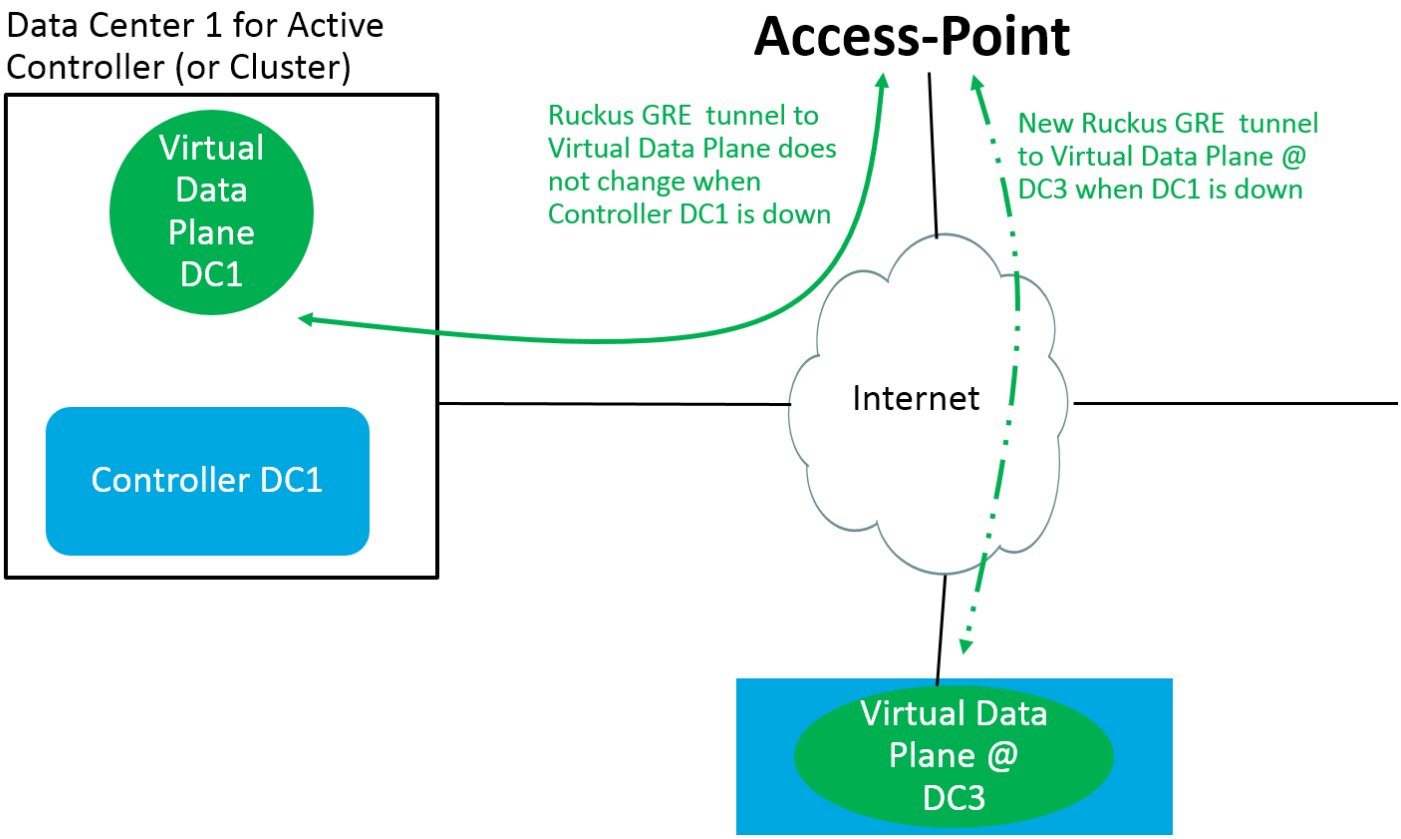
FIGURE 2 Virtual Data Plane SSH Tunnel Failover Between Different Controllers (or Clusters)



AP Ruckus GRE Tunnel Failover Between Different Data Planes

After the access point (AP) establishes the SSH tunnel to the controller (or cluster), the AP receives a list of data plane IP addresses (or data interface IP addresses of the virtual data plane). The AP then establishes the Ruckus GRE tunnel with the first IP address in the list. When a controller goes down, the AP maintains the same tunnel with the data plane until the data plane goes down.

FIGURE 3 AP Ruckus GRE Tunnel Failover Between Different Data Planes



How to Deploy the Ruckus Controller and Data Plane (or Virtual Data Plane) with Cluster Redundancy

Case 1A: Active-Standby Virtual SmartZone with a Single Virtual Data Plane

In this deployment case, the active cluster (controller) has only one virtual data plane.

FIGURE 4 SSH Tunnel Between Access Point and Controller at each Data Center

In Active-Standby Cluster redundancy with Virtual Smart Zone, by design intent, the Standby Cluster does not have any Virtual Data Plane

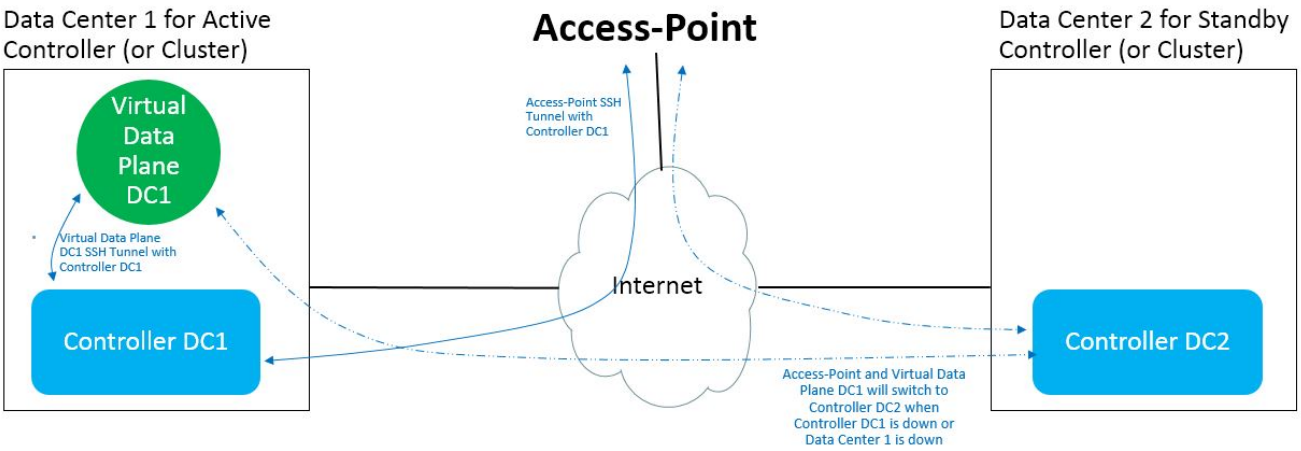
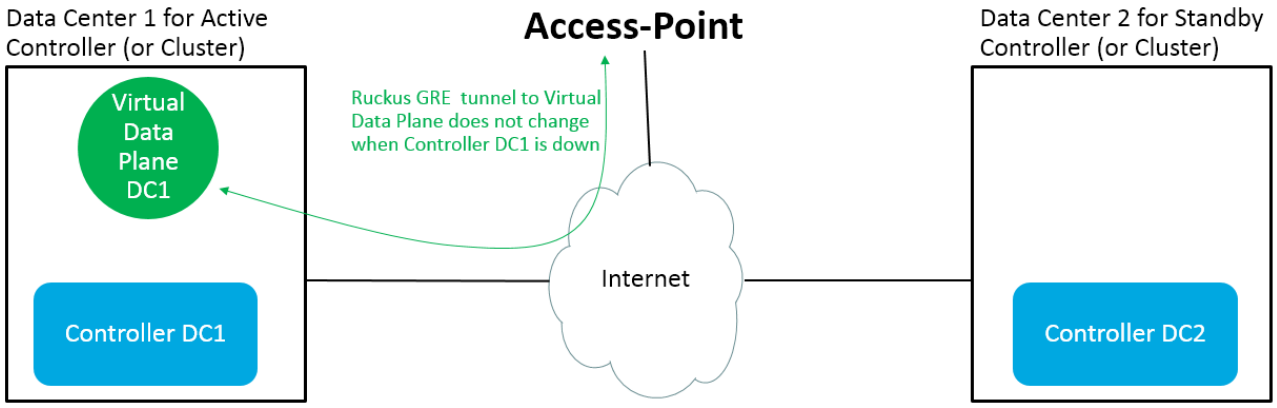


FIGURE 5 Ruckus GRE Tunnel Between Access Point and Virtual Data Plane

In Active-Standby Cluster redundancy with Virtual Smart Zone, by design intent, the Standby Cluster does not have any Virtual Data Plane



CAVEATS: In this topology, when Data Center 1 is down, Access Point does not have Ruckus GRE Tunnel and WLAN SSID is down

Case 1B: Active-Standby Virtual SmartZone with Multiple Virtual Data Planes

In this deployment case, another virtual data plane is added to the cluster for redundancy. The second virtual data plane should not be installed in the same data center with the first virtual data plane.

FIGURE 6 SSH Tunnel Between Access Point and Controller at each Data Center

In Active-Standby Cluster redundancy with Virtual Smart Zone, by design intent, the Standby Cluster does not have any Virtual Data Plane

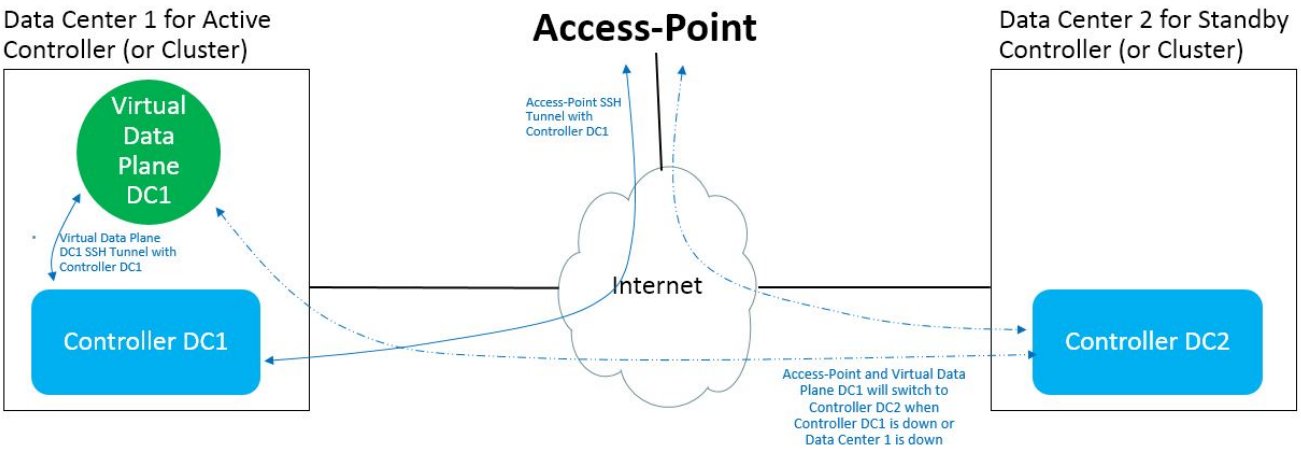
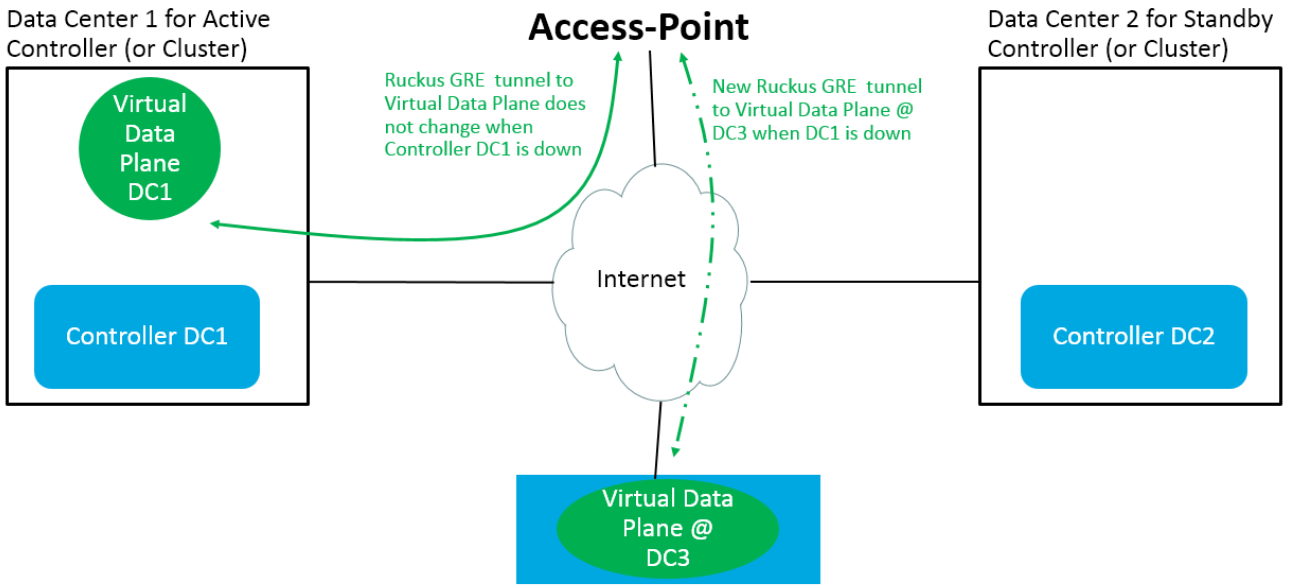


FIGURE 7 Ruckus GRE Tunnel Between Access Point and Multiple Virtual Data Planes

In Active-Standby Cluster redundancy with Virtual Smart Zone, the Standby Cluster does not have any Virtual Data Plane



CAVEATS: In this topology, all deployed Access-Point have Ruckus GRE tunnel either with Virtual Data Plane DC1 or Virtual Data Plane @ DC3

Case 2A: Active-Active Virtual SmartZone with a Single Virtual Data Plane

FIGURE 8 SSH Tunnel Between Access Point and Controller at each Data Center

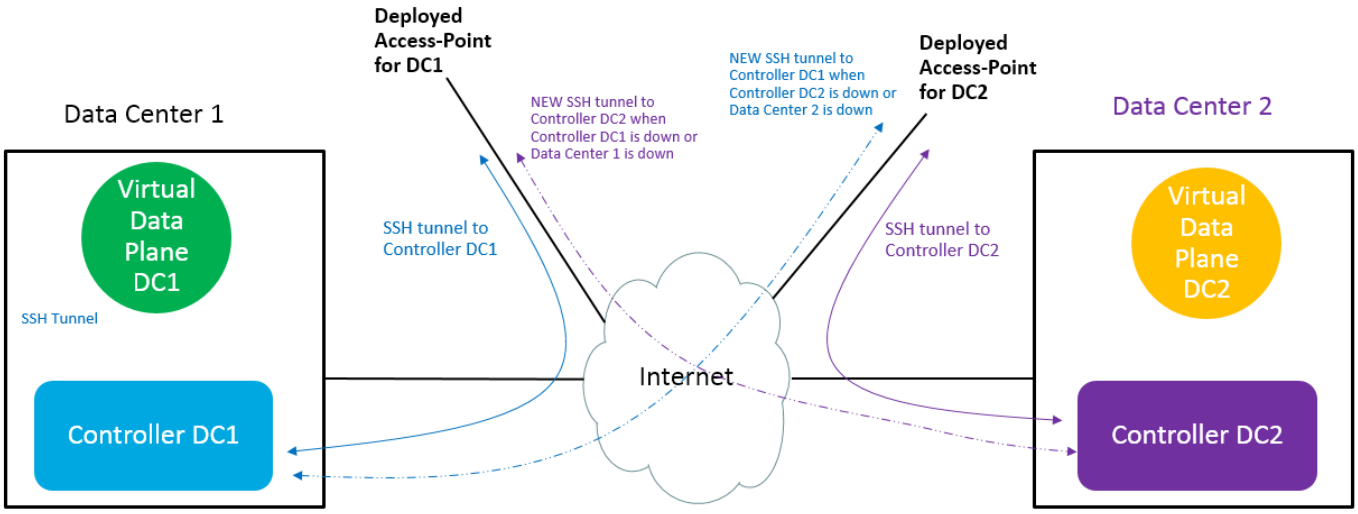


FIGURE 9 SSH Tunnel Between Virtual Data Plane and Controller at each Data Center

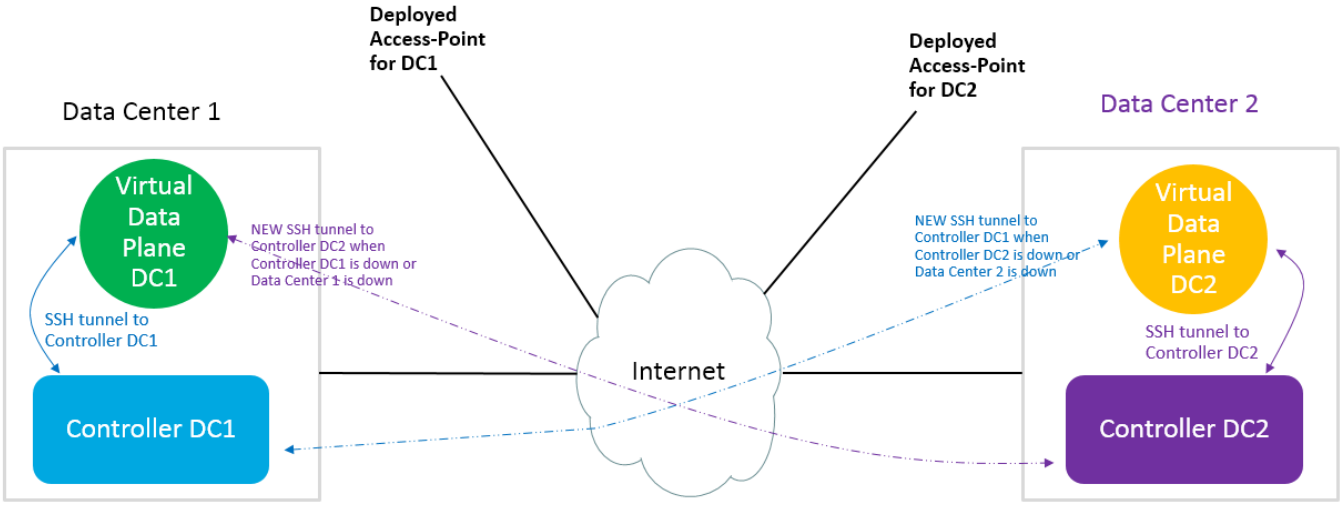
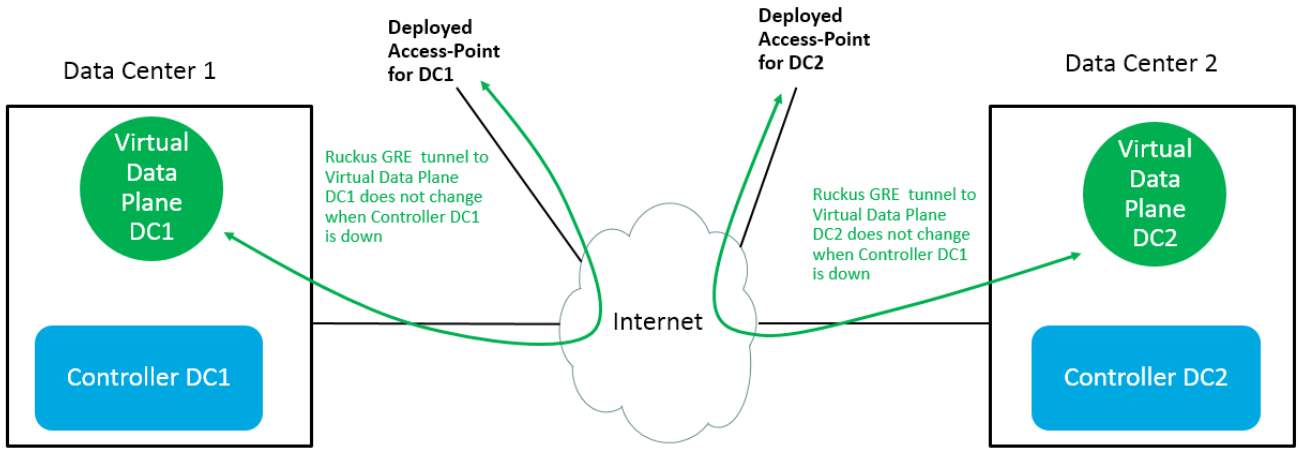


FIGURE 10 Ruckus GRE Tunnel Between Access Point and Virtual Data Plane at each Data Center

In Active-Active Cluster redundancy with Virtual Smart Zone, each Active Cluster has its own Virtual Data Plane with Zone Affinity profile. The Zone Affinity Profile is needed to assign a group of Virtual Data Plane to each Data Center



CAVEATS: In this topology, when Data Center 1 is down, Access Point does not have Ruckus GRE Tunnel and WLAN SSID is down. However, the AP SSH tunnel will switch to Controller DC2 and WLAN LBO of AP is still in service.

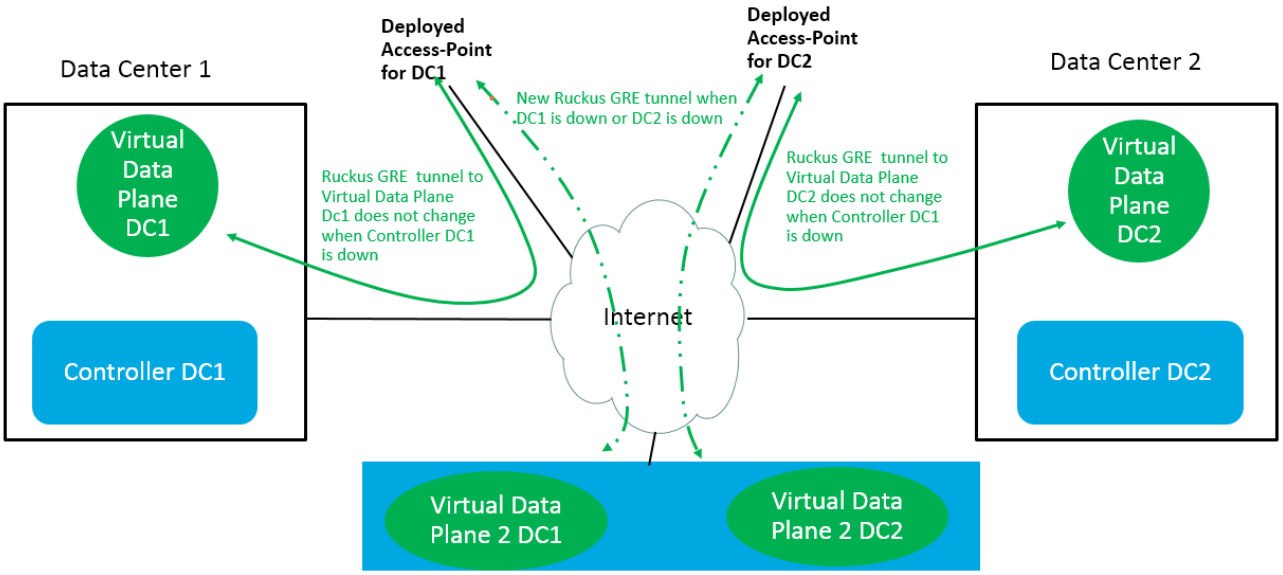
Case 2B: Active-Active Virtual SmartZone with Multiple Virtual Data Planes

NOTE

Refer to Figure 8 on page 11 and Figure 9 on page 11for SSH tunnel examples.

FIGURE 11 Ruckus GRE Tunnel Between Access Point and Multiple Virtual Data Planes at each Data Center

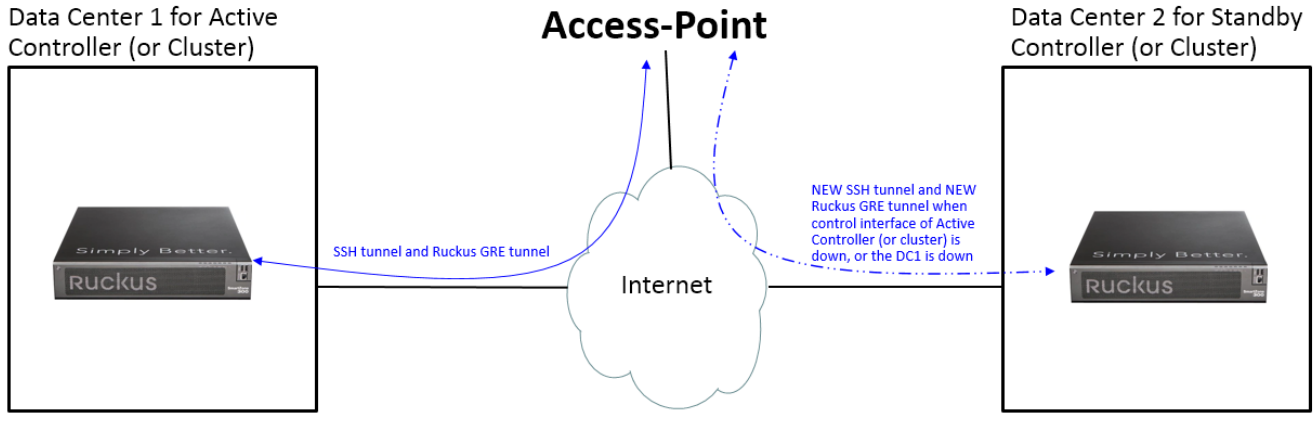
In Active-Active Cluster redundancy with Virtual Smart Zone, each Active Cluster has its own Virtual Data Plane with Zone Affinity profile. The Zone Affinity Profile is needed to assign a group of Virtual Data Plane to each Data Center



Case 3: Active-Standby SmartZone 300

FIGURE 12 SSH Tunnel and Ruckus GRE Tunnel Between Access Point and Active Controller (or Cluster) and Standby Controller (or Cluster)

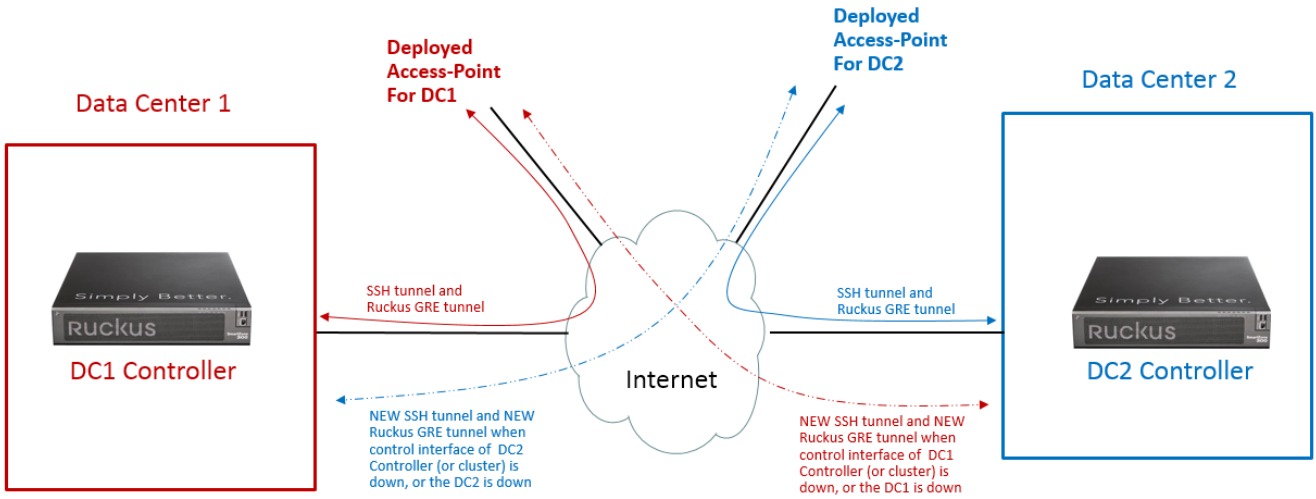
In SZ300 Controller, the Control and Data Plane are communicating on a PCIe bus of the System. Therefore, when SSH tunnel failover happens, Access-Point will also change Ruckus GRE tunnel to the remote SZ300 Data Plane



Case 4: Active-Active SmartZone 300

FIGURE 13 SSH Tunnel and Ruckus GRE Tunnel Between Access Point and each Controller at Different Data Center

In SZ300 Controller, the Control and Data Plane are communicating on a PCIe bus of the System. Therefore, when SSH tunnel failover happens, Access-Point will also change Ruckus GRE tunnel to the remote SZ300 Data Plane



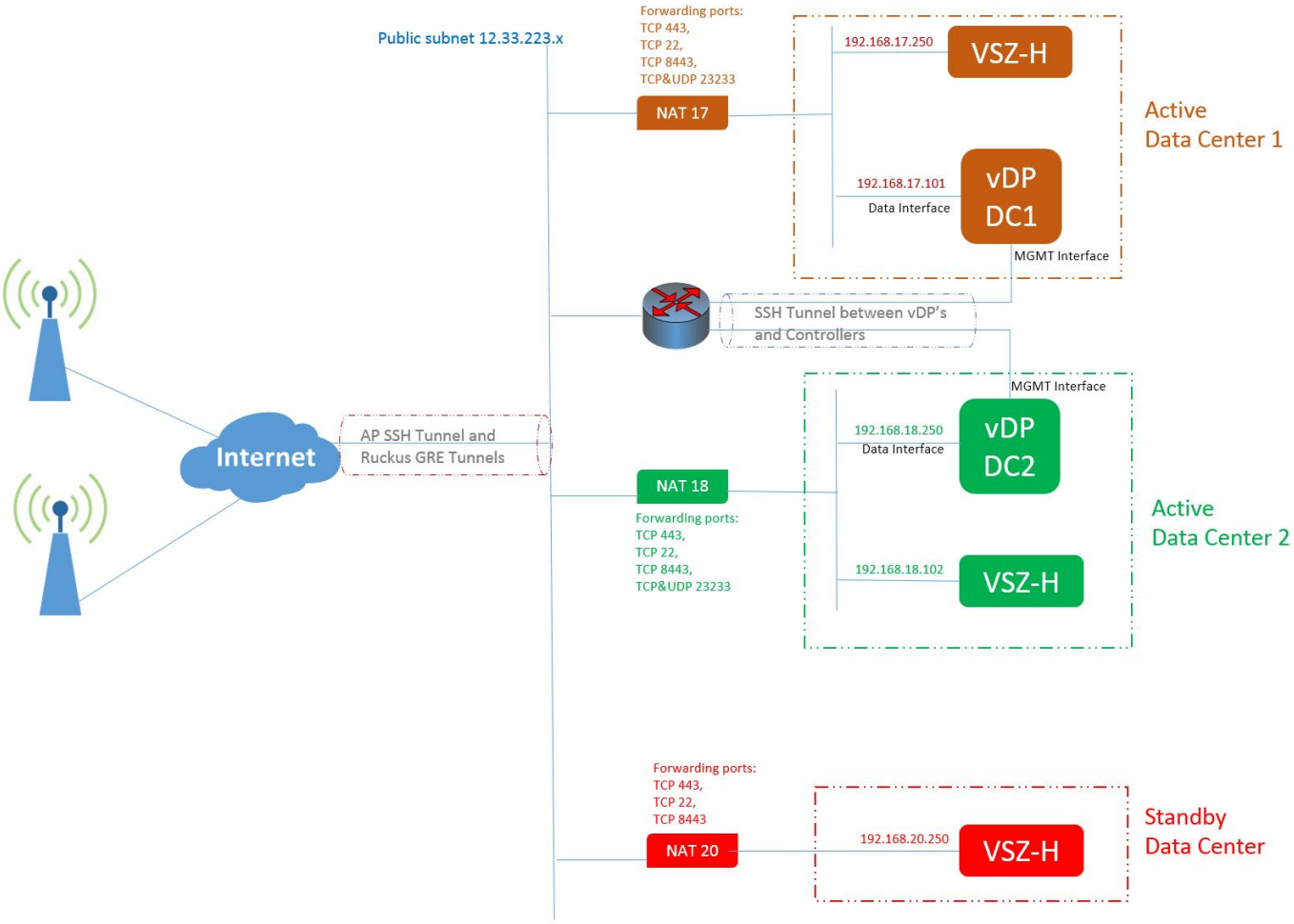
Example Configuration for Cluster Redundancy with Active-Standby

Standby Cluster with Multiple Active Clusters (All Behind NAT Router)

In this type of Active-Standby configuration:

- The active controller (or cluster) at Data Center 1 may have a different configuration than the active controller (or cluster) at Data Center 2.
- The standby cluster has the latest backup configuration of active Data Center 1 and active Data Center 2.
- The standby cluster is in Monitor mode and periodically checks the services at both active clusters every two minutes.
- The standby cluster will switch from Monitor mode to Standby mode after 10 minutes from the time it detects an active cluster down. When the standby cluster is in Standby mode to back up a failed active cluster, it will not be able to back up another failed active cluster.

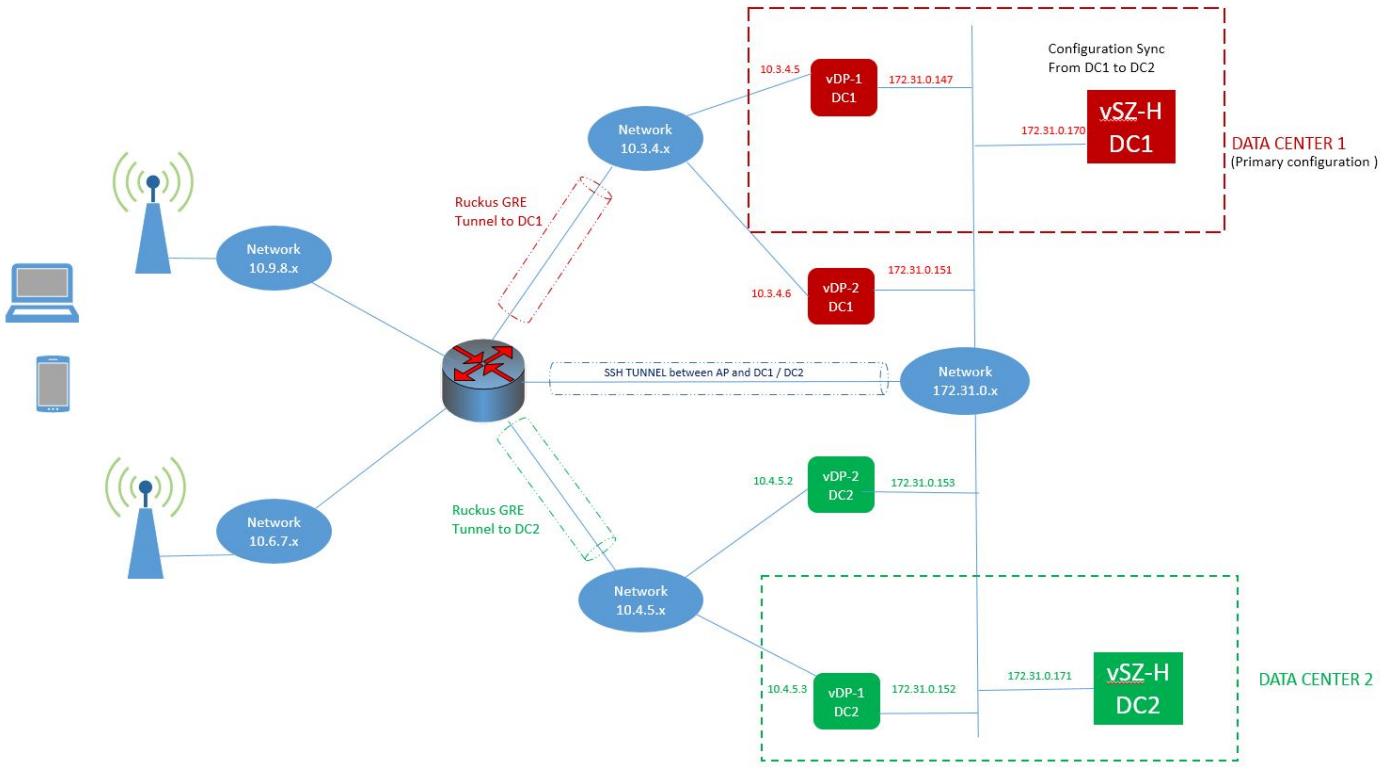
FIGURE 14 Active-Standby Cluster Redundancy with NAT Router Deployment



Example Configuration for Cluster Redundancy with Active-Active

Active-Active Cluster with No NAT Router

FIGURE 15 Active-Active Cluster Redundancy with Multiple Virtual Data Planes



In this configuration, the controller in Data Center 1 has two zones:

- The zone named “DC1” with Zone Affinity that has vDP-1 DC1 and vDP-2 DC1 for all deployed APs for Data Center 1.

  NOTE
  The vDP-2 DC1 should not be installed in Data Center 1. This is because when Data Center 1 is down, vDP-2 DC1 is still available for the Ruckus GRE tunnel from all deployed APs for Data Center 1.

- The zone named “DC2” with Zone Affinity that has vDP-1 DC2 and vDP-2 DC2 for all deployed APs for Data Center 1.

  NOTE
  The vDP-2 DC2 should not be installed in DataCenter 2. This is because when Data Center 2 is down, vDP-2 DC2 is still available for the Ruckus GRE tunnel from all deployed APs for Data Center 2.

AP registration rules are needed for the APs to automatically move to the correct zone when the failover occurs.

Differences Between Active-Active and Active-Standby Cluster Redundancy

TABLE 1 Active-Active Versus Active-Standby Cluster Redundancy

Functions	Active-Active	Active-Standby	Notes
Manage Access Point	All controllers manage access point	Active controller manages access point Standby controller manages access point when active controller is down	
License			
AP Capacity license	Each controller needs a different AP Capacity license	Active controller needs AP Capacity license (full price) Standby controller needs AP-HA license (discount price)	
AP license expiration	Each controller needs a different AP Capacity license	Permanent at active controller A warning message appears at standby controller after 90 days of the AP failover from active controller	
Support license	Each controller needs a different Support PTNR and Support EU license	Active controller needs Support PTNR and Support EU license (full price) Backup controller needs Support PTNR-HA and EU-HA license (discount price)	
vDP Capacity license	Each controller needs a different vDP Capacity license	Active controller needs vDP Capacity license (full price) Backup controller inherits vDP Capacity license from active controller	For Active-Active cluster redundancy, to ensure each cluster can handle the number of failover APs and vDPs when the other active cluster is down, the AP and vDP Capacity licenses at each cluster must be double the number of the registered APs and vDPs in that cluster
vDP feature license	Each controller needs a different vDP feature license	Active controller needs a different vDP feature license (full price) Backup controller inherits vDP feature licenses from active controller	
Number of network interfaces (apply for vSZ-H)	Must be the same	Can be different	
Cluster version AP patches KSP patches	Must be the same	Must be the same	
Controller Model	Must be the same	Active cluster is vSZ-H, standby must be vSZ-H Active cluster is SZ300, standby must be SZ300 because vSZ-H standby does not have data plane If there is no WLAN tunnel with SZ300 deployment, then vSZ-H can be used as backup	Number of NICs of vSZ-H in Active-Standby cluster can be different

TABLE 1 Active-Active Versus Active-Standby Cluster Redundancy (continued)

Functions	Active-Active	Active-Standby	Notes
Number of remote backup clusters	One cluster can be configured to have up to three different backup active clusters	One active cluster can be configured to have only one backup cluster One backup cluster can be configured to back up up to three different active clusters	Backup cluster can only manage one failed active cluster at a time
Cluster communication	None	Backup cluster checks all the services of the active cluster every two minutes	
Cluster mode	Always in active mode to manage AP and provide the services	Standby cluster has two modes: Monitor mode: Periodically checks the services at active cluster Standby mode: Accepting SSH tunnel requests from AP and vDP	
Controller IP list at AP for SSH tunnel			
IP Server list *before* failover	List of internal cluster IP addresses	List of internal cluster IP addresses	
IP Failover list *before* failover	List of remote cluster IP addresses	List of standby cluster IP addresses	
IP Server list *after* failover	List of internal cluster IP addresses	List of standby cluster IP addresses	
IP Failover list *after* failover	List of remote cluster IP addresses	None	
Configuration synchronization mode			
Schedule configuration synchronization	Yes	Yes	
Apply configuration after received backup configuration synchronization	Yes, apply the configuration after synchronization	No, backup configuration synchronization from active will be applied on the standby cluster 10 minutes after the standby changes from Monitor mode to Standby mode	
Configuration change	Configuration change must be applied at a designated active cluster	Configuration change is allowed *only* at active cluster	
Configuration synchronization direction	From a designated active cluster	From active cluster	
Time for AP failover when active controller is down	Takes 3 to 5 minutes to completely failover	Takes at least 25 to 30 minutes to completely failover	
Time for vDP failover when active controller is down	Takes 3 to 5 minutes to completely failover	Takes at least 25 to 30 minutes to completely failover	
Rehome active cluster option	This option is not available	This option is supported in SmartZone 3.6 APs	Rehome AP will apply to vDPs also

TABLE 1 Active-Active Versus Active-Standby Cluster Redundancy (continued)

Functions	Active-Active	Active-Standby	Notes
Switchover cluster option	Need to switch over cluster AP and vDP *separately* When switchover cluster: 1. User can delete AP if AP registration rule is set; otherwise, it is not recommended 2. User should not delete the vDP	This option will be the only option after SmartZone 3.6 is end-of-support	
Upgrade process	One active cluster at a time	Upgrade active cluster first, then upgrade backup cluster	

Caveats and Limitations of Cluster Redundancy

ATTENTION
The following caveats and limitations of cluster redundancy must be reviewed by system engineers and customers before deployment.

Active-Standby Cluster Redundancy

- Standby cluster can back up multiple active clusters, but one at a time.
- Once an active cluster is down, it takes 10 minutes for the standby cluster to change from Monitor mode to Standby mode, which starts accepting SSH tunnel requests from access points and the virtual data plane. The standby cluster then takes an additional 20 minutes to restore the latest backup configuration from the failed active cluster. Total downtime for access points and the virtual data plane is 30 minutes when the active controller (or cluster) is down.

Active-Active Cluster Redundancy

- In each active cluster, the number of AP Capacity licenses and vDP Capacity licenses must be double the number of registered APs and approved vDPs in each cluster.

  For example, if two active clusters have Active-Active cluster redundancy enabled, and each cluster has 50 registered APs and 2 approved vDPs, the customer must purchase 100 AP Capacity licenses and 4 vDP Capacity licenses for each active cluster to support a failover.
- Configuration synchronization *must be* from a selected active cluster.
- Depending on whether the remote controller is behind a NAT router, it takes 3 to 5 minutes for access points and the virtual data plane to fail over to another active controller (or cluster) when the current active controller (or cluster) is down.

Summary

Redundancy is a key part of SmartZone clustering, the benefits of which apply broadly to any network deployment. Cluster redundancy benefits include:

- All controllers in Active-Active cluster redundancy provide service at the same time.
- In Active-Active cluster redundancy, different controllers at different data centers, or different regions, can back up each other.
- Access points (APs) and virtual data planes (if the deployment uses Virtual SmartZone and the virtual data plane) can use a backup controller when their primary data center is down.
- In Active-Standby cluster redundancy, multiple controllers (or clusters) can share the same backup controllers (or clusters) one at a time.

Active-Active and Active-Standby cluster redundancy (including the virtual data plane) are designed for cases where users cannot have all the controllers in the same cluster. Reasons for this may include:

- Bandwidth limitations on the cluster link.
- SZ300 or vSZ-H with three NIC controllers has a cluster interface on a different network and cannot use a Layer 2 link to reach the other controllers.
- A controller needs to manage different regions separately from other controllers.
- A backup controller (or cluster) is available for different controllers (or clusters).
- Multiple one-node clusters back up each other.

Whether to use Active-Active or Active-Standby cluster redundancy will depend on the specific network architecture, data flows between nodes, and bandwidth and latency. Careful planning is recommended before instituting any design to ensure all requirements are met.

> **NOTE**
> In the case of Active-Active cluster redundancy and the virtual data plane, SmartZone 5.1 or later is required on each controller.

© 2019 ARRIS Enterprises LLC. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com