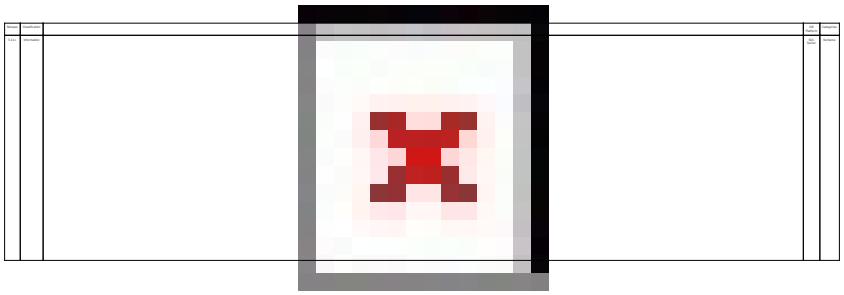
Azure: Kerberos Authentication for ScaleArc configured in Active-Passive mode using Azure Loadbalancer

Abhijit Dhumal - 2017-10-14 - 0 Comments - in Functionality, Internals, and Docs

Azure: Kerberos Authentication for ScaleArc configured in Active-Passive mode

using Azure Loadbalancer



Prerequisites:

Make sure you have the following prerequisites to successfully configure Kerberos

authentication for ScaleArc in an active-passive HA mode using Azure Load Balancer:

Two AMI instances launched with ScaleArc image

AD/KDC, DNS, and SQL servers

Azure instances setup in a single domain

AD, KDC, DNS (with reverse lookup) and NTP servers configured

Configuration can broadly split into the following steps:

Join the ScaleArc nodes to the AD domain as a Machine Account

Configure ScaleArc in Active-Passive HA

Configure ScaleArc for Kerberos

Set up ScaleArc Machine account for Delegations

Provide database access

Create a kerberized cluster in ScaleArc

Verify Kerberos Authentication Offload

The following section discusses each step in detail.

Step 1: Join the ScaleArc nodes to the AD domain as a Machine Account:

Join both the ScaleArc nodes to the Windows AD Domain as a Machine Account. Please refer

this KB article for the necessary steps.

Step 2: Configuring ScaleArc in Active-Passive HA

This KB article outlines the steps for configuring ScaleArc in Active-Passive configuration

using Azure Load Balancer.

Step 3: Configuring ScaleArc for Kerberos: Set up Service Principal Name (SPN) for ScaleArc

SPN is a unique identifier for a service on a network that uses Kerberos authentication. It consists of a service class, a host name, and a port. To create an SPN, use the "SetSPN" command line utility.

From the power shell, set up the Service Principal Name for ScaleArc on AD:

Log into the Active Directory server as a user with domain administrator's privileges.

From the power shell, set the service principal name for ScaleArc on AD. Remember to specify the port correctly.

As we do not have VIPs in Azure, we will register the SPNs with "ALL IP" i.e the Hostname of the ScaleArc Primary Node.

Setspn -A MSSQLSvc/<ScaleArc Hostname>.<domainname>:<port>
<domain\ScaleArc hostname$>

Example
C:\>setspn -A MSSQLSvc/scale-test.krbs.com:1433 krbs\scale-pri$
Note: <port> is the port number on which the Cluster will be running.

If you wish to create an AlwaysON cluster in ScaleArc, Set the SPN of the AG Listener.

Setspn -A MSSQLSvc/<AG LISTENER_Hostname>.<domainname>:<port><domain\domain admin user>
Example

```
C:\>setspn -A MSSQLSvc/aglsnr.krbs.com:1433 krbs\cls
```

Create a DNS entry with the Internal IP address of the Azure LB and its Hostname.

Set the SPN for the Azure LB:

Setspn -A MSSQLSvc/<Azure LB Hostname>.<domainname>:<port> <domain\ScaleArc

hostname$>

Example

```
C:\>setspn -A MSSQLSvc/azurelb.krbs.com:1433 krbs\scale-pri$
```

Step 4: Set up ScaleArc Machine account for Delegations:

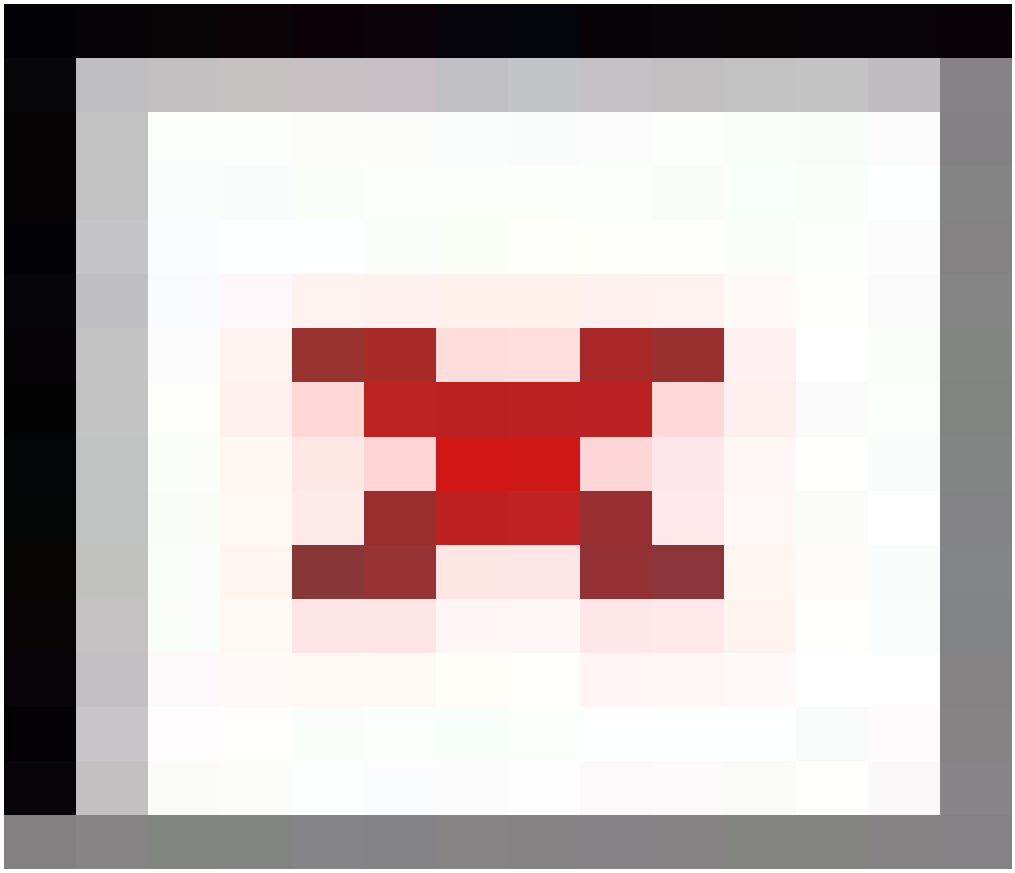
On the domain controller, access the Active Directory Users and Computers console.

In the console tree, under Domain name, click Computers.

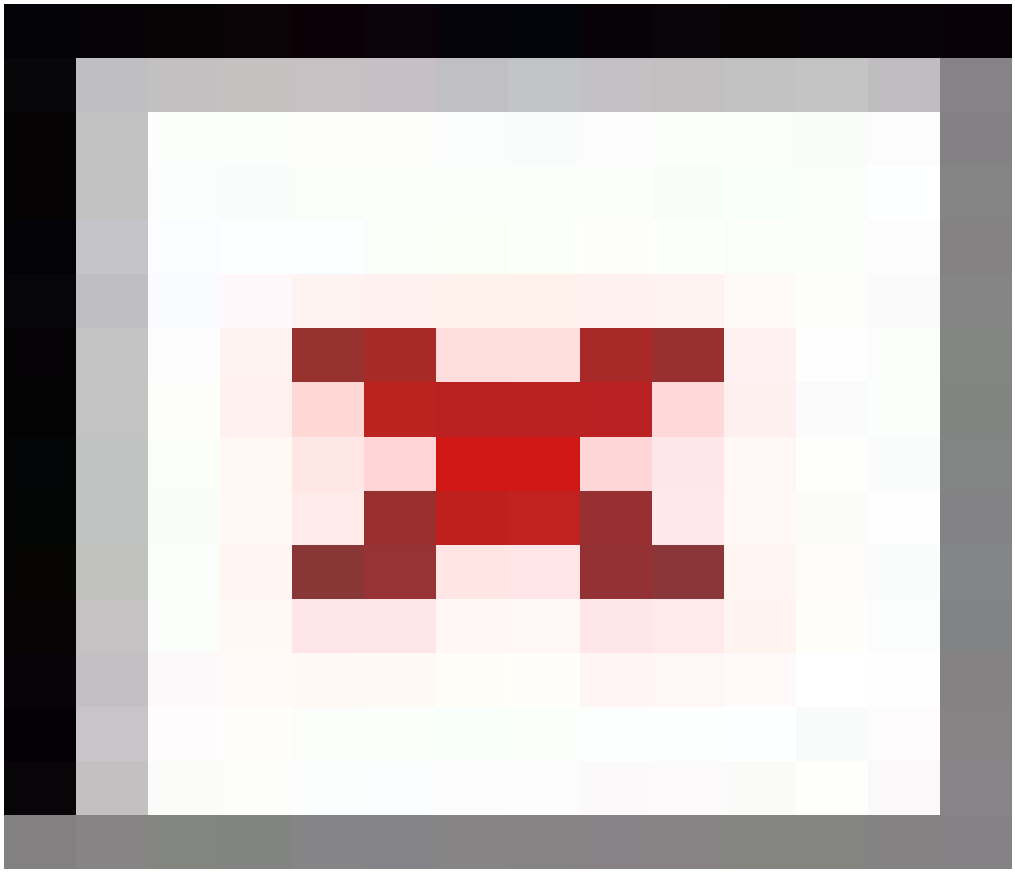
Right-click the ScaleArc server, and then click Properties.

On the Delegation tab, click Trust this computer for delegation to specified services only.

Click Use any authentication protocol.

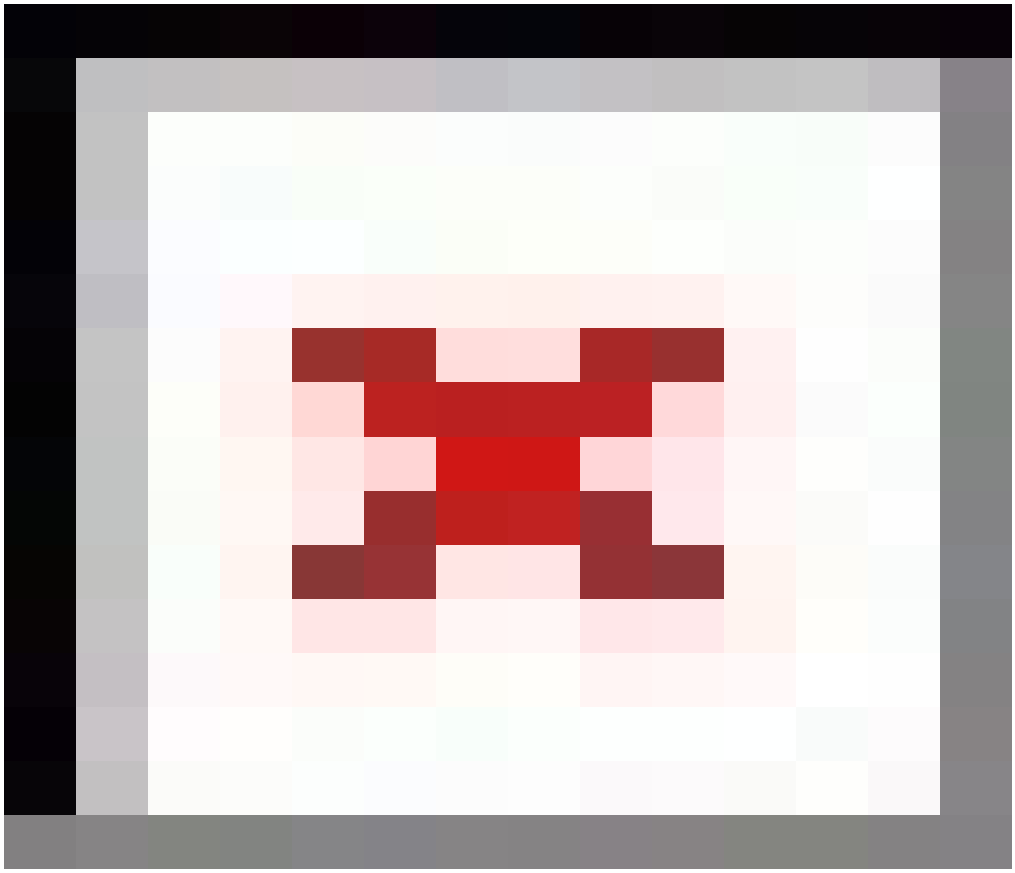


Click Add, and then click Users and Computers.



Enter the domain user that has the necessary credentials to start and stop SQL services; then, Select All DB serverer entries with Instance name and with Port number and Click OK.

From the Delegation tab, click Add. Then, click Users or Computers and enter the machine account name of the ScaleArc primary machine (for example, scale-pri$). Click Check Names and OK.



Select the HOST and the MSSQLSvc service for the ScaleArc Primary node Hostname created earlier. Press the Control key to select multiple entries. Click OK.

1

The entries appear on the Delegation tab. Click Ok.

1

Now the ScaleArc is setup for Kerberos delegation.

Step 5: Provide database access

This is a two-step process:

Set up SQL Server for authentication with the ScaleArc's machine account

Configure database access

Grant access to ScaleArc's machine account:

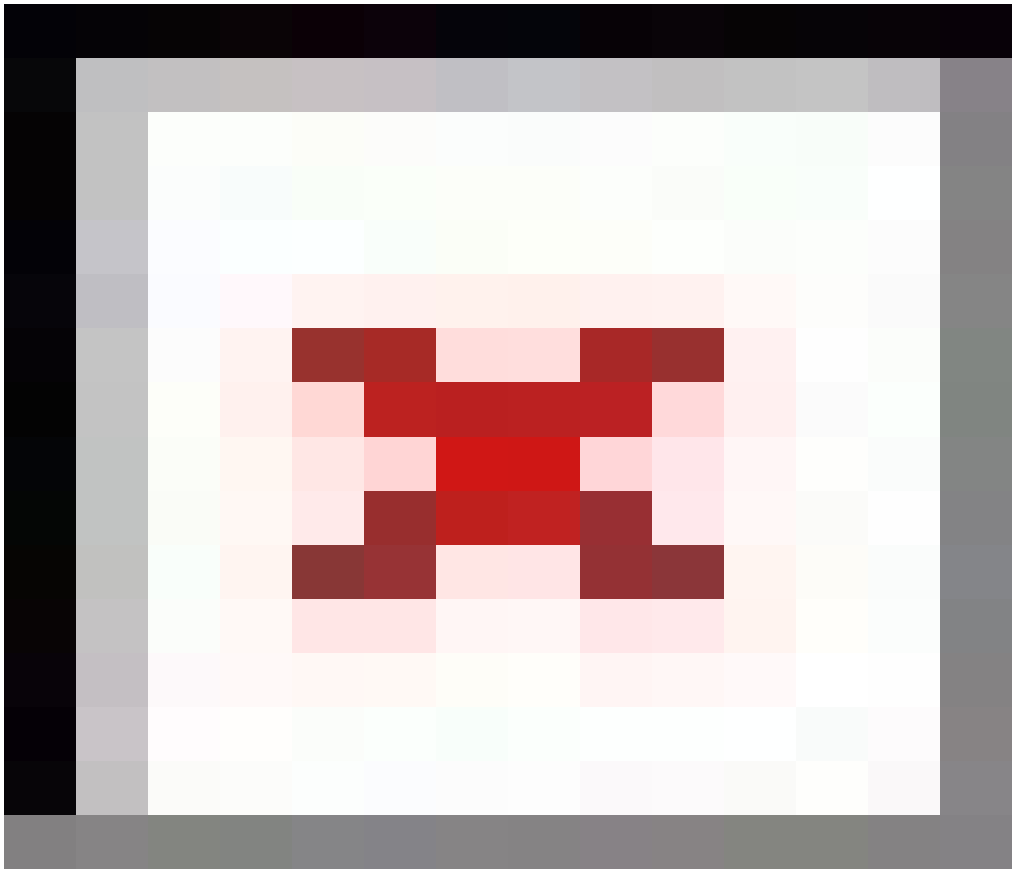
Follow these steps to grant minimum privileges to ScaleArc on SQL Server:

From the machine running SQL Server, log in to SQL Management studio.

Connect to the server.

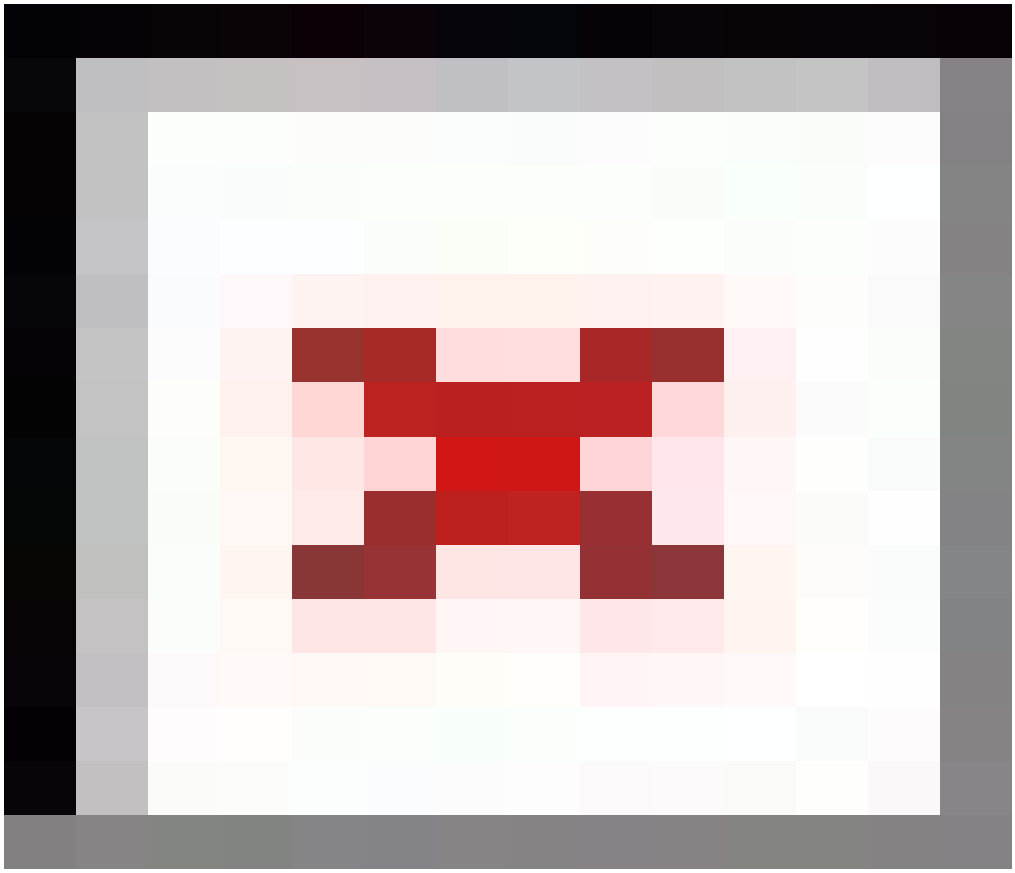
Log in.

Locate Security > Logins > New Login. Remember to add $ at the end of the login name.



Select the user. Right-click on properties.

Under the Explicit tab, select the following permissions.(View Any Definition, View Server status.)



Click OK.

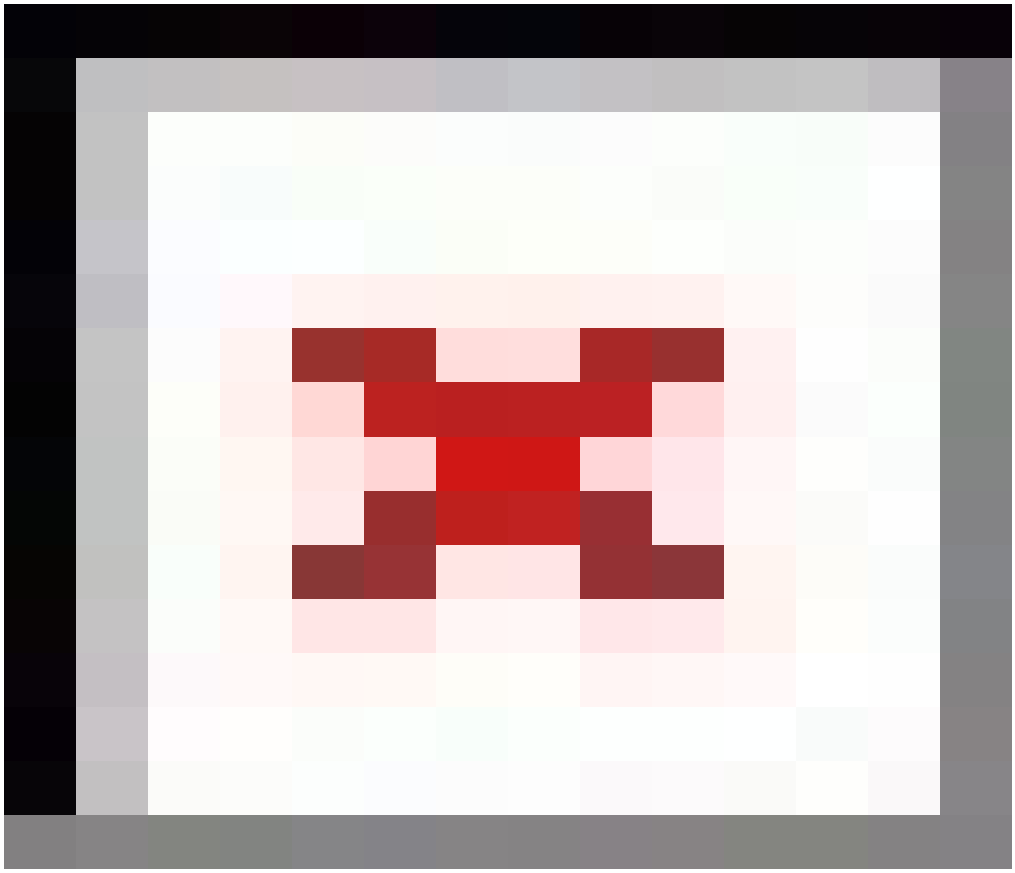
Step 6: Create a kerberized cluster in ScaleArc.

You are now ready to create a Kerberized cluster in ScaleArc. Follow these steps to create a

cluster:

On the ScaleArc dashboard, click the Clusters tab > Add Cluster button.

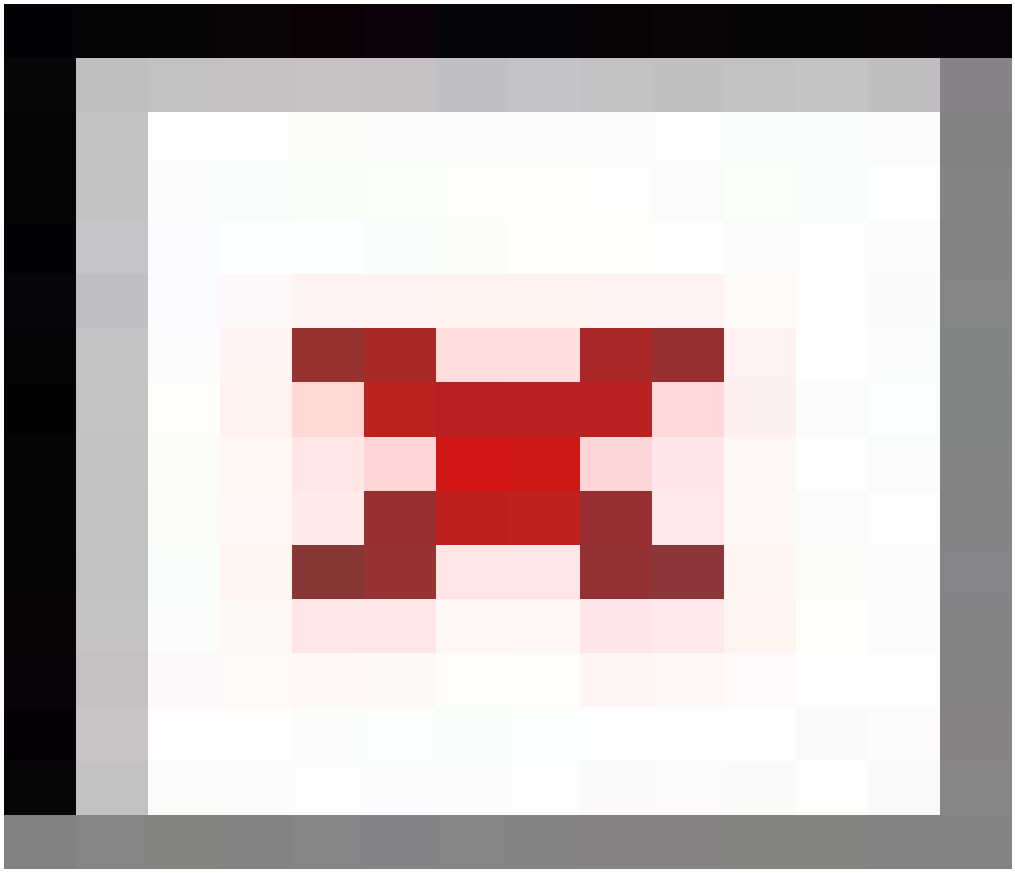
Locate the Network section. This is the first panel on the Create Cluster screen.



Fill in the fields with valid information

Select the "All IPs" for the field labeled Cluster Virtual IP Address and Outbound Virtual IP Address.

Locate the Database Access section. This is the second panel on the Create Cluster screen.



Configure the fields as follows:

Field/Button	Description	Default/User input
Use Kerberos authentication for ScaleArc administration	Ensures that the entire cluster is running in a complete, Kerberos-authenticated mode. Note that when you select this option you do not need to enter username and password. Make sure you have set up minimum database privileges. If you deselect this option, you need to provide a username and password for ScaleArc to establish and administrate database connection using NTLM. Click here to review ScaleArc settings for Kerberos.	This option is pre-selected if you have configured ScaleArc to join the domain as a machine account.
Start Cluster After Setup	Determines if the cluster automatically goes live, following setup. A selected checkbox results in a live cluster at setup. When deselected, you need to start the cluster manually.	Default: Checkbox is pre-selected. Select/Deselect checkbox.

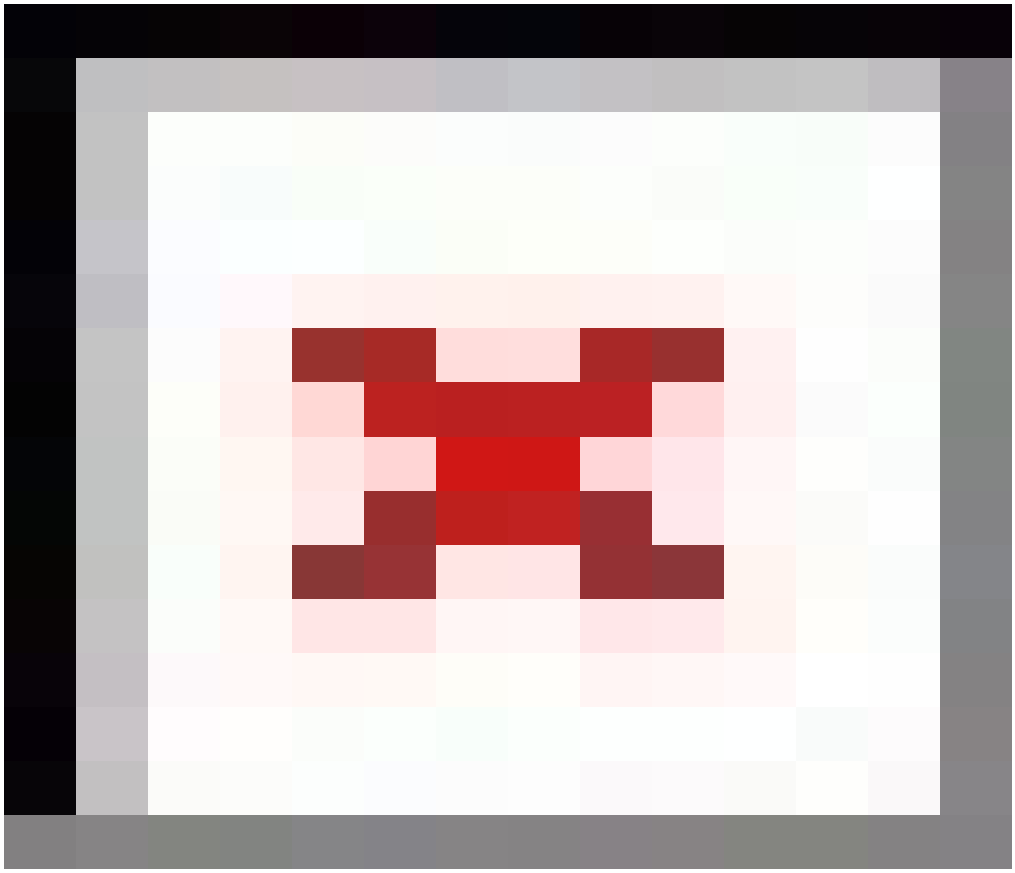
Next, configure SSL (optional) and database servers for the cluster.

Step 7: Verify Kerberos Authentication Offload

A fully-Kerberized cluster has the Kerberized Authentication Offload button set to ON when ScaleArc joins AD as a machine account and the Database Access option for Kerberos is

pre-selected. Click here to review ScaleArc settings for Kerberos.

Click Clusters > Status > Cluster Settings in the ScaleArc dashboard.



Select the ScaleArc tab.

Locate the Kerberos Authentication Offload button. Note that it is ON.

Reference:

The following page in the administrator’s guide outlines the steps for configuring ScaleArc

for Kerberos: Create a Kerberized cluster.

If you are experiencing issues with ScaleArc or with any of it's features, please contact

ScaleArc Support. We are available 24x7 by phone at 855 800 7225 or +1 408 412 7315.

For general support inquiries, you can also e-mail us at support@scalearc.com.

Permalink:
https://support.scalearc.com/kb/articles/4433

Tags

Active-Passive mode using Azure Loadbalancer

Azure kerberos

Azure LB kerberos