Monitor Amazon Databases

SQL Secure lets you connect with Amazon instances in the following cases:

- Log in to RDS instance from On-Premise servers using On-Premise Directory service account user credentials (Windows Authentication).
- Log in to SQL Server installed on EC2 machines, from on-premise using a private IP address and Windows Authentication credentials on on-premise Directory service account.
- Read registry values and query Windows Operating System through WMI queries of EC2 machines from On-Premise using On-Premise Directory service account user credentials.

Manage Microsoft Active Directory with Amazon AWS

AWS Directory Service lets you run Microsoft Active Directory (AD) as a managed service. For more details, please go through AWS documentation

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_getting_started.html

Setting up a VPN Tunnel to connect to Amazon instances

VPN tunnel is required to access SQL Server on Amazon EC2 and RDS from on-premise AD using windows authentication. Setting up VPN tunnel requires to essential steps:

Configuring AWS:

You can find the steps to configure the AWS in the following link:

https://docs.aws.amazon.com/vpc/latest/userguide/SetUpVPNConnections.html

Configuring the Local Network:

This configuration mainly depends on the gateway device used. Identify the approach to create tunnel according the network being used. AWS provides the local gateway side configuration for many networks, like fortinet, as an example:

https://docs.aws.amazon.com/vpc/latest/userguide/SetUpVPNConnections.html

https://docs.aws.amazon.com/vpc/latest/adminguide/fortinet.html

Connecting to your existing AD infrastructure

To use your existing AD infrastructure with AWS Managed Microsoft AD, trust relationship has

to be established between both domains. Use the following documentation:

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_tutorial_setup_trust.html

After establishing trust, you can connect to AWS EC2 instances using your on-premise AD.

Note: To log in into SQL Server on EC2 instance or RDS from on-premise using windows

authentication, you can add on-premise active directory users to SQL Server Security -> Logins.

Authorizing Inbound Traffic for Your AWS security group

Security groups let you control and identify the kind of the traffic that can reach to your instance. Your default and created security groups include default rules that do not enable you to access your instance from the Internet. To enable network access to your instance, you must allow inbound traffic to your instance. To open a port for inbound traffic, add a rule to a security group that you associated with your instance when you launched it.

Adding a rule to a security group for inbound TCP traffic over IPv4 (AWS console)

Choose Instances in the navigation pane of the Amazon EC2/RDS console. Select your instance and look at the Description tab. A list of the security groups related with the instance displays. Choose view inbound rules to display a list of the rules that are in effect for the instance.

- In the navigation pane, choose Security Groups. Select one of the security groups associated with your instance.
- In the Details pane, on the Inbound tab choose Edit. In the dialog, choose Add Rule and then TCP from the type list.
- In the source field, choose Custom and specify the public IPv4 address of your computer or network in CIDR notation.
- Save the changes.

Some important ports to open:

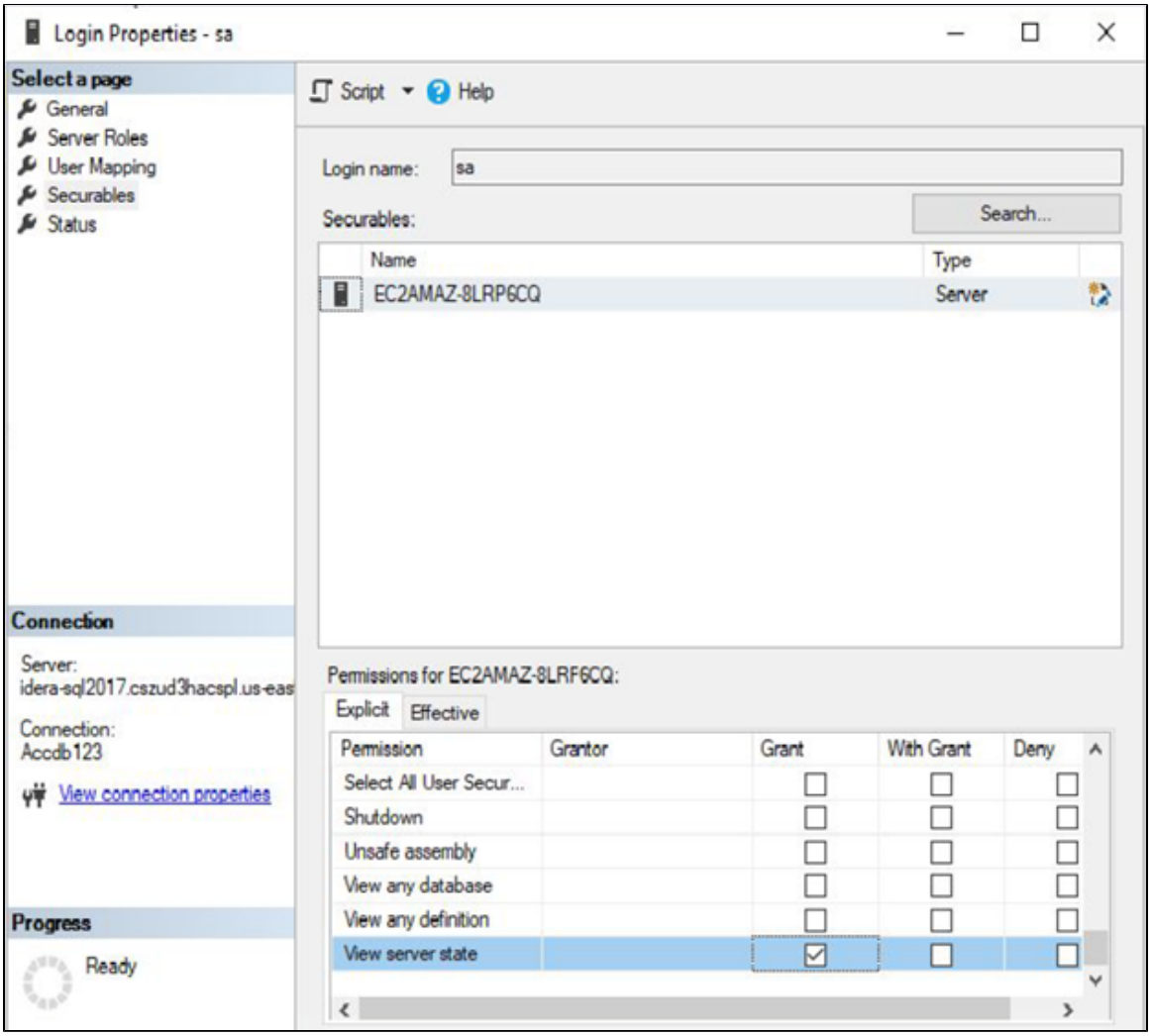
- TCP Port where SQL Server is installed. Default port is 1433.
- TCP Port for WMI. 135
- TCP Port for SMB. 445
- TCP Port for SQL Server Browser service. 1434
- TCP Port for RPC 49152-65535

Note: Note that other ports may be required depending on the respective environment.

Permissions to RDS for SQL Server log in

The login used for RDS for SQL Server needs permissions, right click on the log in and select Properties, then choose Securables and check Grant for:

- View server state
- Alter trace


Login Properties - sa
Select a page
General
Server Roles
User Mapping
Securables
Status
Script
Help
Login name:
sa
Securables:
Search...
Name
Type
EC2AMAZ-8LRP6CQ
Server
Connection
Server:
idera-sql2017.cszud3hacspl.us-eas
Connection:
Accdb123
View connection properties
Progress
Ready
Permissions for EC2AMAZ-8LRF6CQ:
Explicit
Effective
Permission
Grantor
Grant
With Grant
Deny
Select All User Secur...
Shutdown
Unsafe assembly
View any database
View any definition
View server state