

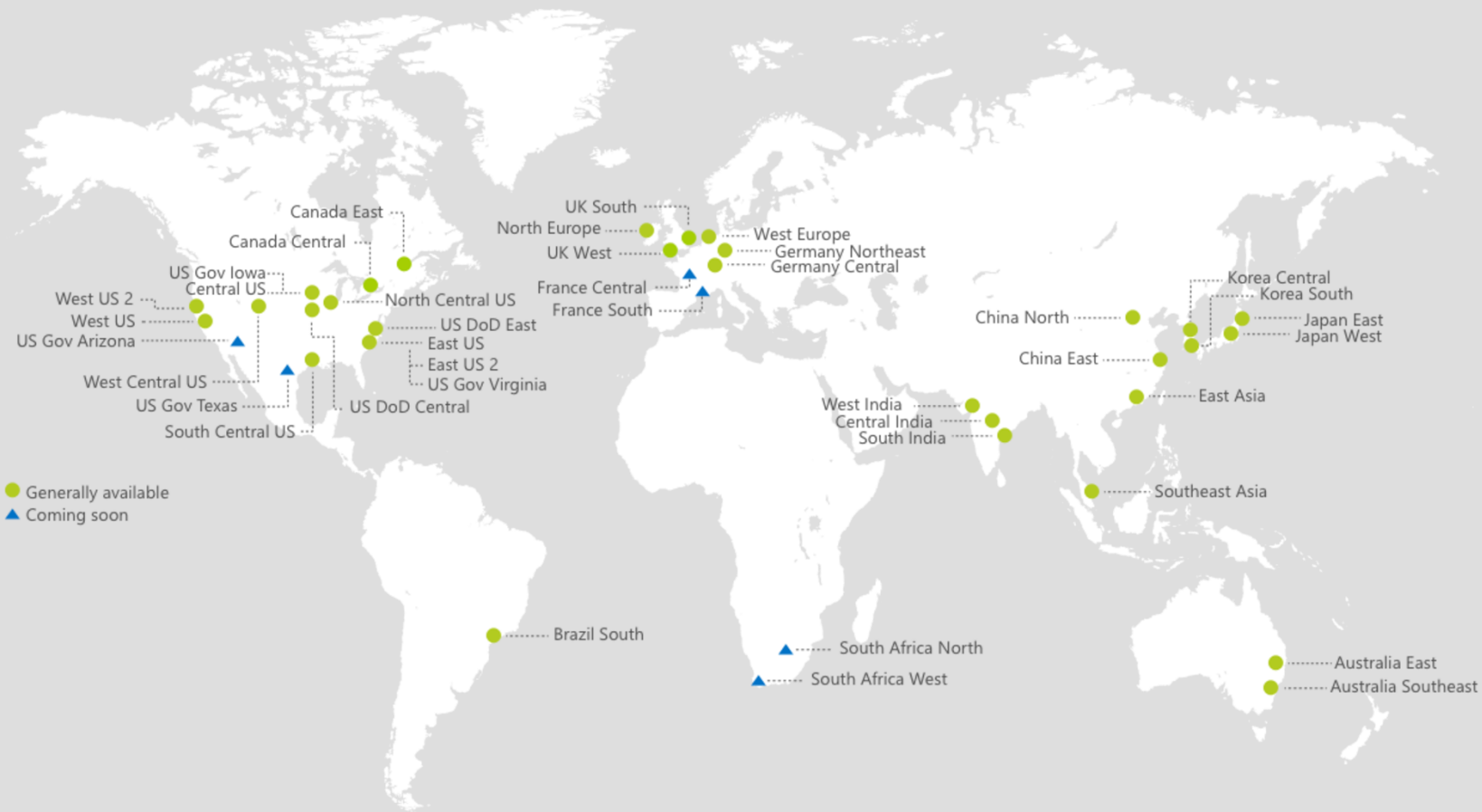
# Azure SREBot - more than a chatbot - an intelligent bot to crush mitigation time

Cezar Guimaraes

cezarg@microsoft.com

@cezargbr

# 40 Azure regions, more than any cloud provider



compliance offerings. More than any other cloud provider



of Fortune 500 companies use the Microsoft Cloud



new Azure customer subscriptions per month

# Platform Services

### Security & Management

- Portal
- Azure Active Directory
- Azure AD B2C
- Multi-Factor Authentication
- Automation
- Scheduler
- Key Vault
- Store/Marketplace
- VM Image Gallery & VM Depot

### Services Compute

- Cloud Services
- Service Fabric
- Batch
- RemoteApp

### Integration

- Storage Queues
- BizTalk Services
- Hybrid Connections
- Service Bus

### Media & CDN

- Media Services
- Content Delivery Network (CDN)

### Web and Mobile

- Web Apps
- API Apps
- Mobile Apps
- Logic Apps
- API Management
- Notification Hubs

### Developer Services

- Visual Studio
- Azure SDK
- VS Online
- App Insights

### Data

- SQL Database
- Data Warehouse
- DocumentDB
- Redis Cache
- Azure Search
- Storage Tables

### Analytics & IoT

- HDInsight
- Machine Learning
- Stream Analytics
- Data Lake
- Data Factory
- Event Hubs
- Data Catalog
- IoT Hub
- Mobile Engagement

### Hybrid Operations

- Azure AD Health Monitoring
- AD Privileged Identity Management
- Domain Services
- Backup
- Operational Analytics
- Import/Export
- Azure Site Recovery
- StorSimple

# Infrastructure Services

### OS/Server Compute

- Virtual Machines
- Container Service

### Storage

- BLOB Storage
- Azure Files
- Premium Storage

### Networking

- Virtual Network
- Load Balancer
- DNS
- Express Route
- Traffic Manager
- VPN Gateway
- App Gateway

Datacenter Infrastructure (40 Regions)



Customer obsessed  
Crush downtime minutes

Share wisdom

# Incident response activities











M-800

a.k.a  
SREBot

Available

2 Participants

Wednesday, May 17, 2017

who is oncall for compute

3:45 PM

The current shift for Compute team is:  
Shift Name: Oncall Shift  
Primary: Compute Engineer1  
Email: [compute.engineer1@microsoft.com](mailto:compute.engineer1@microsoft.com)  
Work Phone: 1234567890  
Cell Phone: 0012345678  
Home Phone: 0012345670

3:45 PM

Backup: Compute Engineer2  
Email: [compute.engineer2@microsoft.com](mailto:compute.engineer2@microsoft.com)  
Work Phone: 0123456789  
Cell Phone: 0001234567  
Home Phone: 0012345670

Last message received on 5/17/2017 at 3:45 PM.



Available

 2 Participants

Saturday, June 3, 2017

engage compute

6:52 AM



It seems as though you forgot to give me a/an **Incident Id**  
Can you tell me what the **Incident Id** is?  
If you do not have an incident Id and need to create a ticket say "create ticket" to make one

6:52 AM

create ticket

6:52 AM



It seems as though you forgot to give me a/an **title, severity**  
Can you tell me what the **title** is?  
Please put the title in quotes ex: "Ticket title"

6:52 AM

"test ticket" sev-2

6:52 AM



Got it! I've successfully submitted an engagement request to Compute for IncidentId 123456.  
You can check the status of this request by looking under the notifications tab  
here: <http://ticketingsystem?incident=123456/engage>

6:52 AM

Last message received on 6/3/2017 at 6:52 AM.



Available

2 Participants

Wednesday, May 17, 2017

how is compute doing in west us?

3:54 PM



Here is the filtered dashboard showing health of Compute in region 'West US': <http://computehealth?region=westus>

3:54 PM

Last message received on 5/17/2017 at 3:54 PM.











**SKYNET**

NEURAL NET-BASED ARTIFICIAL INTELLIGENCE

a.k.a

Crisis Management Intelligence  
Engine

Available

2 Participants

Wednesday, May 17, 2017

show active bridges

4:28 PM



There are **3 active\*** sev 0-2 bridges. Here is the list:

4:28 PM

- Incident #[123456](#) | [Join Bridge](#) | Sev-1 | Test Incident 1
  - Incident #[123457](#) | [Join Bridge](#) | Sev-2 | Test Incident 2
  - Incident #[123458](#) | [Join Bridge](#) | Sev-2 | Test Incident 3
- \*An active bridge has at least one participant.

Last message received on 5/17/2017 at 4:28 PM.



Available

2 Participants

Wednesday, May 17, 2017

who is oncall for sql

5:12 PM

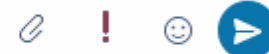


For Tean Name `SQL` I found multiple options to choose from.

5:12 PM

- SQL - Team 4
- SQL - Team 1
- SQL - Team 3
- SQL - Team 2

Last message received on 5/17/2017 at 5:12 PM.



NLP

Available

2 Participants

Wednesday, May 17, 2017

what are the datacenters in europe north

4:18 PM



NorthEurope has the following datacenters in it

4:18 PM

- NorthEurope DC 1
- NorthEurope DC 2
- NorthEurope DC 3
- NorthEurope DC 4

Last message received on 5/17/2017 at 4:18 PM.



# Pro-active Knowledgeable



## SRE Bot VM Health Assessment

Based on information SRE Bot has for this incident on **DC1**, from **3/24/2017 1:02:20 AM UTC** to **3/24/2017 1:32:20 AM UTC**, it looks like

- **2 clusters** have a total of **12 reboot events** from **8 distinct VMs**.
- It was found that there is a total of **3 distinct subscriptions** associated with the rebooted VMs. These include **2 external subscriptions** and **1 internal subscription**.

Below are the 2 clusters:

<a href="#">Excel</a>	<a href="#">Copy</a>	Show <input type="text" value="10"/> entries	Search: <input type="text"/>
Cluster	Count of distinct VM(s) that rebooted	Total VM reboot count	
Cluster1	5	7	
Cluster2	3	5	

Showing 1 to 2 of 2 entries

[Previous](#) [1](#) [Next](#)

Below are the 3 subscriptions:

<a href="#">Excel</a>	<a href="#">Copy</a>	Show <input type="text" value="10"/> entries	Search: <input type="text"/>		
Subscription Guid	Customer Name	Subscription Type	Count of distinct VM(s) that rebooted	Total VM reboot count	Subscription Status
1-1	Cyberdine systems	External	2	4	ACTIVE
2-2	Sky.net	External	2	3	ACTIVE
3-3	T-888 Co	Internal	1	5	ACTIVE

Showing 1 to 3 of 3 entries

[Previous](#) [1](#) [Next](#)



How we did it

# Reactive Architecture

News



Weather



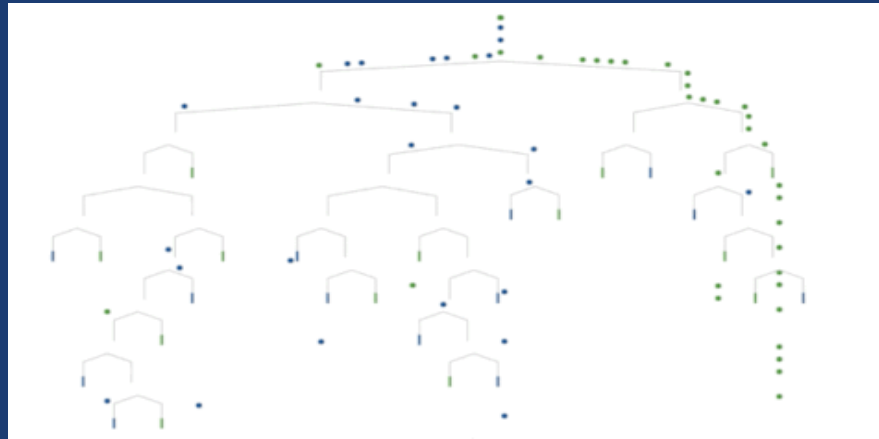
Telemetry



Logs



Intelligence Engine



REST API

Skype



Teams



Slack



PowerShell



Bots

Human



Machine



DC Tool



Network Tool



.....



# Extensibility

```
{  
  "service": "compute",  
  "aliases": [ "compute", "azure compute" ],  
  "dashboardurl": "https://computehealth",  
  "dashboardtype": "comprehensive",  
  "planetype": "none",  
  "readorwrite": "none"  
},
```

# Plugin

Intent  
Required entities  
Execute method

```
public interface BotPlugin
{
    string Description { get; }
    string ExampleNlpPhrase { get; }
    PluginEntities Entities { get; }
    PluginIntent Intent { get; }
    Task<string> Execute(Message message, IEnumerable<MessageEntity> entities, string topic);
}
```

---



who is on call in foo service

who is **on call** in foo service  
intent = oncall

who is on call in foo service  
plugin requires => service name

who is on call in foo service

Available

2 Participants

Wednesday, May 17, 2017

get me the chatlog

4:06 PM



It seems as though you forgot to give me a/an Incident Id  
Can you tell me what the Incident Id is?

4:06 PM

12345

4:06 PM



Here is the link for chat log: <http://BotChatLog&INCIDENTNO=12345>

4:06 PM

Last message received on 5/17/2017 at 4:06 PM.



Not so simple 😞

what are the datacenters in west us

what are the clusters in datacenter XX2

is datacenter XX2 in west us

list all datacenters

Domain : Context : Topic



what are the datacenters in west us region

what are the datacenters in west us region

Fleet : Datacenter : region

what are the datacenters in `west us` region

What next?

# Intelligence Engine extensions

## More and more intelligence

# Q&A

Cezar Guimaraes  
cezarg@microsoft.com  
@cezargbr