Universal Computer Management (ARC for Servers) Planning & Deployment

Description

A system management and control solution, using the Microsoft ARC for Server's platform, with support for Windows and Linux OSs located on a broad set of virtualisation providers (Windows Server Hyper-V, AS HCI, KVM, Nutanix and VMware), physical hardware platforms and non-Microsoft cloud providers.

The solution allows system maintenance and administration to be performed without requiring direct connection into the system under management or using traditional management protocols that commonly require additional setup or are not suited to multi-platform, multi-location management.

As part of the solution, all computers under management appear and are treated as Azure native resources, enabling Azure native management capabilities, including (but not limited to); policy, security, log analytics' and RBAC, to be applied.

Additional extensions may be optionally deployed to enable workload or application-specific capabilities (extensions or capabilities utilising extensions may incur additional fees).

Features

- Deployment and maintenance of ARC agents onto (supported) target computers.
- Configuration of the Windows operating system:
  - Management of operating system features via an Azure-hosted instance of Windows Admin Center.
    - OS-level management features are dependent on the Windows Admin Center plug-in feature set provided within Azure.
  - Remote access to VM console via RDP.
- All operating systems:
  - View and control system compliance status.
  - View and deploy system updates and patches.
  - Track and monitor changes in software (deployment), files, system registry settings and operating system services (demons).
  - Control access to the resource via Azure policy and RBAC.
  - Configure and manage Automation workflows (automation workflows run against the Azure object (ARM resource), not the local machine operating system.

Optional features

The universal machine management solution (ARC for Servers) enables the following capabilities. Implementing these services will require additional configuration (including technical knowledge of the base technology) and incur additional fees.

Acuutech can implement the optional features as part of its solution portfolio (additional fees will apply).

- Anti-virus and malware protection.
- Proactive security monitoring and protection.
- Patching and updating, including dynamic “intelligent” update deployment.
- Logging, log analytics and auditing.

Supported Platforms

- A virtual machine or physical (hardware) server running the following OS:
  - Windows Server Windows Server 2012 R2, 2016, 2019, and 2022 (including Server Core)
  - Ubuntu 16.04, 18.04, and 20.04 LTS (x64)
  - CentOS Linux 7 and 8 (x64)
  - SUSE Linux Enterprise Server (SLES) 12 and 15 (x64)
  - Red Hat Enterprise Linux (RHEL) 7 and 8 (x64)
  - Amazon Linux 2 (x64)
  - Oracle Linux 7

Virtual machines running all supported OSs are supported when operating on the following infrastructure platforms:

- Microsoft Windows Server Hyper-V
- AS HCI
- VMWare
- Nutanix
- KVM or derivative hypervisor
- Public cloud platforms

Un-Supported

The following locations are not supported (as VMs on these systems are already defined as Azure native objects).

- VMs running within Microsoft Azure
- VMs running on Azure Stack HUB
- VMs running on Azure Stack Edge

Requirements

- Windows-based OSs – Administrator (or equivalent) level access to all OS features.
- Linux-based OSs – Root (or equivalent) level access to all OS features.
- Support for TLS 1.2 or later within the OS of the machine to be placed under management.
- Outbound connection to the Internet via TCP port: 443 (HTTPS).
- An Azure tenant.
- An account with the following tenant permissions:
  - To onboard machines: Azure Connected Machine Onboarding or Contributor role in the resource group.
  - To read, modify, and delete a machine: Azure Connected Machine Resource Administrator role in the resource group.
  - To generate onboarding script: Minimum a member of the Reader role for that resource group.

Limitations

- No more than 800 Azure objects (items) within a single resource group.
- ARC agent connection via proxy configuration is not supported.