ServiceNow Cloud Management:
Accelerating and Strengthening Cloud Development and Operations
Introduction

Today’s modern organizations are turning to the cloud to deliver IT applications and services. The cloud offers the promise of unparalleled speed and agility—the touchstone of modern IT organizations. Whether IT, like DevOps, is vertically integrated or has horizontally layered development and operational teams, it has to respond rapidly to business needs. In this way, IT becomes an equal partner in breaking down the barriers to innovation. The cloud is a key enabler for this.

However, agility and effective governance are often in conflict today. While speed is paramount, IT teams also need end-to-end process discipline to ensure quality, security, and compliance. The cloud is built for speed, while manual IT processes are not. This duality can act as a huge impediment on enterprises, defeating the purpose of Agile development, delivery, and operations.

For example, consider a private virtualized environment that is tightly controlled by IT administration. Development teams need to spin up development and test environments in minutes, but they often wait days for a VM to be provisioned. Not only does this result in delays, it is also a major cause of VM sprawl. Users are reluctant to release cloud resources in case they need them again in the future. This leads to capacity issues as well as an increasingly chaotic private virtualized environment.

On the other hand, public clouds such as Amazon Cloud and Microsoft Azure allow developers and other end users to provision cloud infrastructure directly, bypassing internal IT processes. This is highly attractive, particularly since technologies such as CloudFormation can create complete cloud environments. However, because public clouds can be effectively ungoverned, individual users often create their own accounts and provision their own resources. This leads to significant challenges.

First, because there is no centralized control over what resources users can provision, public cloud costs can run out of control. It’s not unusual to consume an entire year’s cloud budget in six months or less. Users also forget to deprovision resources when they are no longer required, creating sprawl just like in private clouds.

Second, because each user creates their own cloud infrastructure, there is no standardization or version control. For instance, users may share CloudFormation templates, but there is no centralized management that ensures this is done. This creates significant risks—for example, there’s no guarantee that development, test, and production environments comply with the right technical and security policies.

Third, account management and access control become major issues. Multiple cloud accounts become increasingly difficult to administer. On the other hand, multiple users often need to access the same cloud infrastructure using a single account, but there is no consistent role-based access control to manage what individual users can do.
In reality, however, organizations often use both public and private clouds. In this hybrid model, there is no unified framework for security, provisioning, configuration, optimization, and service assurance. This greatly increases the complexity of managing hybrid environments, as there is no single system of record, consistent operating framework, or common security model. This greatly increases the complexity of managing hybrid environments, and increases operational costs, as employees need to be trained and become proficient in an expanding set of cloud vendors and technologies. It can also lead to vendor lock in as development and operational processes become tied to a single cloud's capabilities.

On the other hand, any hybrid cloud management solution needs to support the full depth of each cloud offering. While it must provide a common management framework and consistent processes, it must not take a “least common denominator” approach—for instance, it shouldn’t just support common capabilities across different vendors’ VMs. Enterprises want to use the full power of each cloud environment—for example, Amazon’s virtual datacenters, subnets, and security policies. Any solution that limits capabilities to a common subset is doomed to fail.

Furthermore, the need for a common management framework is not just a cloud issue. The cloud is an enabling infrastructure, but ultimately IT delivers business services and applications. Any framework for managing cloud-based business services needs to start with the service itself and manage the cloud as part of that service. Approaches that manage isolated cloud resources, rather than end-to-end services, simply create more silos. To be truly agile, IT organizations need to break down these silos, not build new ones.

Ultimately, you need to know how to create a unified operational model for the cloud that:

- Preserves and enhances the agility of public clouds while addressing standardization, cost, and security issues
- Provisions private clouds and virtualized environments on demand, making them as fast and easy to use as public clouds
- Creates a single system of record and consistent operating model in multivendor or hybrid cloud environments while still exposing the full capabilities of each cloud
- Addresses not just cloud infrastructure but complete business services that run in the cloud

**Introducing ServiceNow Cloud Management**

ServiceNow Cloud Management lets you rise to these challenges. It dramatically accelerates provisioning of public and private cloud infrastructure and managed services, while providing consistent management of cloud resources and business services. With ServiceNow Cloud Management, you can:

- Provision and configure your standardized cloud infrastructure and complete business services and give development teams powerful self-service capabilities that enhance agility, while providing a structured environment that ensures quality, security, and compliance
- Create a single system of record for your public and private cloud infrastructures and the business services that use them
- Discover existing cloud infrastructure resources and business services—and how they relate to each other—bring them under consistent management
- Enhance security and governance through auditable processes and role-based access control
- Resolve cloud infrastructure and business service issues with powerful event and business service management features
- Manage public cloud costs, including allocating costs and detecting underutilized/stranded resources
With ServiceNow Cloud Management, administrators create standardized, version-controlled cloud infrastructure services and offer these to users through the ServiceNow Service Catalog.

ServiceNow Cloud Management provides comprehensive support for Amazon cloud resources and managed services and is designed to evolve seamlessly as these resources and services evolve. It supports private VMware clouds and can also be extended to manage other public and private cloud vendors, delivering a future-proof cloud management solution.

### On-demand cloud infrastructure services

With ServiceNow Cloud Management, administrators create standardized, version-controlled cloud infrastructure services and offer these to users through the ServiceNow Service Catalog. When users open the Service Catalog, they see a list of these services alongside all of the other IT services they normally access. They simply select the service they want, enter appropriate parameters, and submit the request. ServiceNow then automatically provisions the service in real time. These services can range from individual Amazon EC2 instances or VMware VMs to complete Microsoft Azure cloud resources and Amazon CloudFormation stacks—which can include virtual datacenters, subnets, security policies, S3 buckets, and managed services.

![Figure 1: A LAMP stack in the ServiceNow Service Catalog](image)

While the ServiceNow Service Catalog lets users create cloud resources easily, it is much more than a portal. It is a managed access point for these services, creating a consistent way of provisioning multiple cloud environments, including hybrid public/private cloud architectures. It also delivers security and compliance through role-based permissions and auditable workflows. In addition, it links cloud provisioning into broader IT operations. For example, it automatically raises an incident when a provisioning request fails. In other words, the Service Catalog provides the agility that DevOps needs, while offering the visibility and control that IT governance demands.

![Figure 2: Entering parameters for a cloud infrastructure service](image)
When ServiceNow Cloud Management creates, modifies or deletes a cloud service, it records the details of the service in the ServiceNow CMDB updating CIs and relationships to correspond to the configured service.

**AWS CloudFormation stacks**

To define an AWS CloudFormation service, administrators simply need to create a new service catalog item and associate it with a standard CloudFormation template. This can be the URL of an existing template in an Amazon S3 bucket, or the administrator can enter a JSON template directly into ServiceNow. ServiceNow supports all valid CloudFormation templates—there are no restrictions, even for complex architectures such as VPCs with multiple public and private subnets.

**Amazon EC2 instances and VMware VMs**

When ServiceNow connects to an Amazon account, it automatically discovers all of the Amazon Machine Images (AMIs). Cloud administrators can approve selected AMIs and then use these as templates. To add a new Amazon EC2 service to the Service Catalog, the administrator simply needs to create a new catalog item and associate it with an approved AMI.

Similarly, ServiceNow automatically discovers VMware templates on VMware ESX/ESXi servers. Again, administrators can use these to create service catalog items. They can also define available machine configurations based on CPU counts, memory size, and disk size, and add these as choices to the service catalog item.

**Microsoft Azure Cloud resources**

Microsoft Azure Cloud is fully supported through ServiceNow Cloud Management. Once the Azure Cloud account is registered on the ServiceNow Platform, all cloud resources and subscriptions under that account are discovered, and appropriate service relationships are established and maintained in the CMDB. New cloud resources such as simple virtual machines to entire application stacks can be provisioned and managed using the ServiceNow Cloud Management portal. For Azure, the Azure Resource Manager template (ARM) allows the entire application stack to be described as code so it can be versioned and maintained in the source code control system. The Azure Resource Manager template can be used to create an item in Service Catalog and can be exposed to the end user for a one-click self-service provisioning experience.

**Managing cloud services**

Once a user has created a cloud infrastructure service, they can easily modify it by submitting a change request. This includes updating complete application stacks—the user is able to edit the AWS CloudFormation template, or Azure Resource Manager template, and include this with the change request. Users can also make changes to VMware resources—for example, they can modify the memory or disk capacity of a virtual machine.

With ServiceNow, you control which cloud services are under change management. For instance, administrators can put production services under change control while still letting development instantly update development and test services. In both cases, the changes are fully tracked, but ServiceNow only goes through a full change approval process if change management is enabled. Otherwise, it immediately applies the requested change to the cloud infrastructure service.

**Customizing the user experience**

With ServiceNow, you control how much complexity you expose to end users, and which design patterns you make available. Using provisioning rules, UI policies, and custom variables, you can easily customize forms and ask simple questions—like those related to projects or business services, hardware requirements, and questions about whether the provisioned devices will contain personally identifiable information (PII), and whether they will be used for development or production purposes. Based on these answers, ServiceNow automatically provisions requested cloud infrastructure services into existing VPCs and their subnets, along with corresponding security policies and user access rights.
Configuration management

When ServiceNow Cloud Management creates, modifies, or deletes a cloud service, it records the details of the service in the ServiceNow CMDB—updating CIs and relationships to correspond to the configured service. This provides a consistent single system of record for your entire cloud infrastructure—including both public and private clouds.

The ServiceNow CMDB is the backbone of the entire ServiceNow Platform. It provides resource and service information to a wide range of other ServiceNow applications, creating a consistent, service-aware environment. For example, ServiceNow Event Management associates incoming events with corresponding CIs in the CMDB, and uses the relationships between these CIs to correlate events. The CMDB also lets users easily visualize resources and relationships using interactive business service maps.

The ServiceNow CMDB provides comprehensive support for modeling infrastructure and service relationships between Microsoft Azure Cloud resources, Amazon AWS Cloud resources and services—including complete CloudFormation stacks—as well as VMware private cloud resources.

However, the ServiceNow CMDB is not limited to cloud resources. It provides a single system of record for all of the applications, middleware, and other software infrastructure components that run on these cloud resources. This includes application to host mapping, application dependency mapping, and complete business service maps. For example, it can map all of the databases that connect to a specific app server. It can also describe the topology of a complete business service—such as a customer portal, including the specific web servers, storage elements, network connections, and other components that support the service, along with their service-specific relationships.

Figure 3: Partial business service map for LAMP stack with incident overlay

Configuration automation

In addition to tracking cloud infrastructure and business service configuration, ServiceNow also provides configuration automation capabilities. It can automatically configure individual server nodes or groups of nodes based on attributes such as location, associated SLAs, installed software, or any other characteristics. It also provides change control processes on top of this configuration, which can be implemented using the built-in ServiceNow configuration capabilities or by having ServiceNow act as a configuration provider to Puppet or Chef.
Admin, operator, and user and team portals

ServiceNow Cloud Management gives each user an appropriate view of the application based on their configured role in ServiceNow. Admins have oversight and control of system usage, while operators are able to provide support and review change requests. Cloud users have an intuitive portal where they can see all of their cloud resources, including both Amazon and VMware infrastructure. There are individual user portals, as well as team portals. In addition to providing a list of resources, these portals also include a dashboard that shows key statistics about these resources. For instance, the dashboard includes analysis of resources by type, and also identifies underutilized, stranded, and unattached resources. This gives users complete visibility of their cloud environments, while encouraging them to terminate resources they no longer need.

![Cloud Admin portal](image)

Figure 4: Cloud Admin portal

This portal is also the main point of control for cloud resources once they have been created. From the portal, users can issue change requests and extend leases, as well as start, stop, and terminate instances. Users can also take and manage snapshots from the portal and restore virtual servers.

Infrastructure as code

When ServiceNow provisions a cloud infrastructure service, it uses its Orchestration engine. This engine provides version-controlled activities and workflows—for instance, it includes out-of-the-box activities to provision EC2 instances and CloudFormation stacks.

However, ServiceNow Orchestration is not limited to cloud resources. It can configure any type of IT component, including applications, middleware, and other software infrastructure. Because of this, Orchestration is a powerful way of creating infrastructure as code. Using Orchestration, developers can build version-controlled automation packages that:

- Repeatably and accurately configure complete applications and business services
- Automatically configure monitoring systems to support these applications and business services
- Consistently and automatically remediate service impairments
ServiceNow makes it easy to create and share reusable orchestration activities and workflows. Using its graphical Activity Designer, developers can design version-controlled activities without writing code. The Activity Designer leads them through the complete process, including specifying inputs and outputs, defining parsing rules to extract data from payloads, and creating pre- and post-processing scripts if required. It also provides object-oriented design templates that abstract away complexity, promote consistency and simplify ongoing maintenance. The Activity Designer supports a wide range of interface mechanisms, including JavaScript, SSH, PowerShell, SOAP, and REST.

Developers can invoke these automation packages through a web services interface, making it simple to create and configure infrastructure within their code. Alternatively, developers can easily add these activities to version-controlled ServiceNow workflows using a drag-and-drop Workflow Designer. They simply select an activity from a graphical palette, drag it into a workflow, and connect the inputs and outputs. This provides the option of implementing infrastructure as code entirely within ServiceNow, and then invoking this through a single entry point.

With ServiceNow, all of these automation activities are designed to never fail. For example, if you run out of capacity, ServiceNow automatically escalates the issue for human attention. This means that NOC staff do not need to continuously monitor and manage the health of your automation environment.
Federated AWS console access

While ServiceNow makes it easy to create new standardized services to meet specific needs, there are still times when developers may have to “break the glass” and use the native cloud management console. ServiceNow supports this by providing time-limited federated access to the Amazon AWS console. This gives developers the flexibility they need while still providing role-based security and auditability. It also eliminates the administrative overhead of maintaining multiple AWS accounts for individual users.

To do this, ServiceNow uses the AWS Security Token Service (STS). When a user needs console access to a specific AWS account, ServiceNow requests a security token from STS, passing an AWS IAM profile. The IAM profile specifies the actions the user can perform on the console, and the resources they can access. STS then returns the token to ServiceNow, which uses the token to log the user into the console. This provides a single sign-on mechanism—ServiceNow launches the console directly and the user does not have access to the AWS account password.

To enable console access, administrators select a specific Amazon account and associate it with an IAM profile. This causes a corresponding item to appear in the service catalog. By default, there is one IAM profile for all cloud users, but ServiceNow can be configured to provide fine-grained access control, with specific IAM profiles for different roles.

To gain console access, a user simply selects the corresponding service catalog item and submits a request. ServiceNow then obtains the security token and creates a link to the console on the user’s dashboard. Users can also schedule future access for purposes such as planned maintenance. The link remains until the console access period expires, at which time it is removed from the user’s portal.

Cloud discovery

When ServiceNow Cloud Management provisions a cloud infrastructure service, it keeps a complete record of the service in its CMDB. However, it also discovers Amazon, Azure, and VMware cloud resources, along with their relationships. This lets ServiceNow bring cloud resources under management even if they have been provisioned manually—for example, directly through the cloud provider console. This also makes it easy to bring existing cloud accounts into ServiceNow, as well as track any drift in the environment.

ServiceNow typically uses the cloud provider API for infrastructure resource discovery. Public cloud providers like AWS offer additional services such as AWS Config, which provides notification of changes to the cloud resources. Microsoft Azure Cloud offers a snapshot of changes to the resources for a given time period. ServiceNow uses these capabilities to ensure quick and efficient discovery of change to the cloud resources. VMware allows API-based discovery through vCenter APIs.

When ServiceNow discovers new cloud resources or updates to existing resources, it updates its CMDB. This ensures that the CMDB has a complete record of all cloud resources, whether they are provisioned through the ServiceNow service catalog or through the AWS console. It also gives administrators the option of approving discovered changes before they are accepted into the CMDB.

Application and software infrastructure discovery

As well as discovering cloud resources, ServiceNow Discovery can also discover all of the software components running on this cloud infrastructure. It carries out host-based discovery, mapping applications, databases, middleware, and other software components to virtual hosts. In addition, it maps application dependencies, discovering adjacency relationships between software components. ServiceNow also intelligently classifies virtual hosts—for example, it can automatically assign all hosts running web server software to a common web server group in its CMDB.
As well as discovering cloud resources, ServiceNow Discovery can also discover all of the software components running on this cloud infrastructure.

**Service mapping**

ServiceNow can also automatically map complete business services, like customer portals or banking services. Simply given the service access point, such as a URL or queue, it discovers all of the resources and resources that support the service, along with their relationships. This includes both software components and cloud resources. This makes it easy to map the end-to-end topology of an existing cloud-based business service and bring it under management, as well as monitor the service topology for subsequent changes.

**Event Management**

ServiceNow radically simplifies the task of identifying and resolving cloud infrastructure issues. It provides comprehensive event management for both public and private clouds. This includes out-of-the-box integration with Amazon CloudWatch, delivering real-time visibility of Amazon cloud resources and managed services.

In addition, ServiceNow Event Management integrates with other industry-leading IT infrastructure monitoring tools—like Nagios, SolarWinds, and Icinga—and also collects events directly from SNMP-enabled devices. This extends event management above the cloud resource layer, providing a complete solution for entire business services and applications. As noted previously, ServiceNow can also configure these monitoring systems using Orchestration.

ServiceNow Event Management includes a powerful event filtering engine. This deduplicates, normalizes, and correlates events, turning large volumes of raw event data into a small number of precise, actionable alerts. These alerts are shown on configurable event management dashboards, providing a consolidated view of all service-affecting events, including active alerts, affected business services, and associated incidents. ServiceNow can also carry out automated remediation when service-affecting events occur, including opening incidents, retrieving knowledgebase articles, and even reconfiguring infrastructure.

ServiceNow also makes it easy to visualize events in the context of affected business services. It maps each event to its corresponding CI in the ServiceNow CMDB, for instance, an individual cloud resource or software component. It then displays the CIs and relationships that make up the business service on an intuitive business service map, overlaying associated event, problem, and incident data. This makes it easy to see the impact of issues on individual service components, and to see how these issues propagate from component to component.
Managing public cloud costs

In private clouds, capacity is usually the limiting factor. However, public clouds are different. In a public cloud, capacity is virtually unlimited, and therefore cost management is a major issue. It’s not unusual to see budget overruns of 100% or more if cost and usage are not monitored and controlled.

To address this issue, IT and DevOps groups need fine-grained visibility of costs. They need to be able to track down resources to users, cost centers, and even specific applications, business services, and projects. They also need to ensure that resources are deprovisioned when they’re no longer required so they don’t continue to consume budgets.

ServiceNow provides a number of mechanisms to manage Amazon and Azure cloud costs and usage. These include fine-grained billing reports, lease management, and identification of stranded or underutilized resources. Where appropriate, some of these capabilities—such as lease management—are also available for private VMware clouds where they help to manage capacity.

Amazon and Azure cost allocation tagging

When a user orders an AWS resource, like an EC2 instance or CloudFormation stack, or an Azure resource, like an Azure VM or Azure Resource Manager template, via the ServiceNow Service Catalog, they are asked to provide a cost center. They can also provide additional information, such as an associated project, application, or business service. ServiceNow validates this information and then applies corresponding Amazon or Azure cost allocation tags to the resources. It also stores the cost allocation information directly in the ServiceNow CMDB.

Administrators can also tag resources after they have been provisioned. This lets them bring resources under cost management even if they have been provisioned through the cloud provider console. When ServiceNow discovers AWS or Azure resources, it highlights untagged resources—those created through the console—so administrators can tag them. It also reports tag discrepancies, comparing the cost allocation information in the CMDB to the actual AWS or Azure tags it discovers.

Users can also associate VMware resources with a specific business service and/or application. In this case, ServiceNow stores this information in its CMDB where it can be used for purposes such as chargeback.

Amazon and Azure billing and usage reports

ServiceNow collects detailed billing and usage data directly from AWS and Azure public clouds. It uses this data to produce a range of graphs and reports that make it easy to measure resource costs and usage. By combining this data with cost allocation tags, ServiceNow also provides detailed breakdowns by user, cost center, business service, application, or project.

ServiceNow displays this billing and usage information on an interactive dashboard, which can contain several charts and reports. Administrators can filter and group data using multiple criteria, such as tag values, time period, and geographic region. For example, a dashboard could include an analysis of costs aggregated by business service, along with a breakdown of underutilized resources grouped by specific cloud service, like EBS volumes of AWS or Azure SQL on Azure.
ServiceNow has comprehensive lease management capabilities that ensure cloud resources are automatically deprovisioned once they are no longer required.

Administrators can also configure specific billing aggregations, which ServiceNow uses to roll up data on a daily and monthly basis. ServiceNow stores this aggregated data in its database, and makes it available via Web Services. This makes it easy to extract the data and integrate it with other systems for purposes such as chargeback.

**Lease management**

ServiceNow has comprehensive lease management capabilities that ensure cloud resources are automatically deprovisioned once they are no longer required. Lease management is available for Amazon EC2 instances and CloudFormation stacks, as well as for VMware virtual machines.

When users order a cloud service through the ServiceNow Service Catalog, they have to provide a lease period. By default, this is 60 days, but users can decrease this or increase it up to a limit of 90 days.

As the lease expiry approaches, ServiceNow notifies the user who owns the cloud resource. They can then extend the lease by issuing a change request. If the resource is under change management, the request is routed for approval, otherwise it is extended immediately.

If the lease expires before it is extended, ServiceNow automatically pauses the cloud resource. It then waits for a configurable grace period—seven days by default. If the lease has not been extended by the end of the grace period, ServiceNow automatically terminates the cloud service.

Note that ServiceNow does not automatically terminate leases for production cloud services. Instead, it automatically renews the lease and informs the owner that the lease has been updated.
ServiceNow Cloud Management provides this consistent approach across both public and private cloud environments.

Conclusion

Today, organizations are increasingly turning to the cloud to provide business services. The cloud holds the promise of unparalleled agility, allowing IT to dramatically streamline and accelerate development, delivery, and operation of these services.

However, to deliver this promise, cloud environments must be managed effectively. Today, private clouds are often too slow, and public clouds are largely ungoverned. This leads to chaotic environments, quality issues, and rising costs. What is needed is a consistent management approach that preserves and increases agility, while providing a superior level of visibility and control of both cloud resources and the business services that run in the cloud.

ServiceNow Cloud Management provides this consistent approach across both public and private cloud environments. It delivers cloud infrastructure services on demand, manages the entire lifecycle of these cloud resources, and extends above the cloud to manage complete business services. With ServiceNow, IT provisions and configures cloud infrastructure and business services more quickly and accurately, drives down cloud costs, and increases quality. The result is faster development, more robust deployments, and more effective and consistent operations and governance.