TECHNICAL OVERVIEW

NovaCore Connect

Infrastructure & Business Continuity Overview

1. Overview

NovaCore Connect provides access to virtual desktops and applications through an infrastructure environment made up of interconnected access, delivery, compute, directory, and storage services.

Business continuity depends on understanding how these components support one another and how critical services can be restored after an interruption. This overview describes the main infrastructure layers and recovery planning considerations for NovaCore Connect.

Configurations and recovery arrangements depend on the services selected, the customer’s environment, and documented business requirements.

2. Infrastructure Architecture

NovaCore Connect brings together user access, desktop and application delivery, and supporting AWS infrastructure.

User access

Users connect from supported desktop computers, laptops, or mobile devices. Available access methods depend on the user’s device, connection, and the services configured for the environment.

Access and delivery

Parallels components provide access to NovaCore Connect’s desktop and application delivery services. The role and connection sequence of each component depend on the deployed configuration.

AWS infrastructure

AWS provides underlying resources that support service delivery:

- Amazon EC2 provides compute resources for virtual desktops, applications, and supporting services.
- Active Directory provides identity and authentication services used to manage access to desktops, applications, and other resources.
- Amazon FSx provides managed file storage for workloads that require shared access to files and application data.

These components depend on one another. Recovery planning should account for those dependencies and the sequence required to restore services.

3. Business Continuity Considerations

Continuity planning begins by identifying the services that matter most to business operations and the infrastructure they depend on.

Planning may include:

- Identifying critical desktops, applications, and supporting services.
- Mapping dependencies among identity, networking, compute, storage, and application delivery.
- Setting restoration priorities.
- Defining who coordinates recovery and who validates restored services.
- Documenting the procedures, access, and resources needed during recovery.

The appropriate plan depends on the environment and the business requirements for each service.

4. Backup and Recovery Approach

Veeam Backup & Replication is the planned technology for meeting backup and recovery requirements for selected workloads.

The design should account for:

- Which workloads and data are included in protection.
- Backup frequency and retention requirements.
- Backup storage and access controls.
- Recovery infrastructure and locations.
- Dependencies and priorities for restoring services.
- Procedures for validating restored systems and data.

Backup and replication capabilities depend on the selected configuration and protected workloads. They do not, by themselves, guarantee uninterrupted service or a specific recovery timeframe.

5. Recovery Objectives: RTO and RPO

Recovery objectives help organizations define their recovery needs.

Recovery Time Objective (RTO)

RTO is the target timeframe for restoring a service after an interruption. It helps teams prioritize restoration and plan the people, procedures, and infrastructure required.

Recovery Point Objective (RPO)

RPO is the maximum acceptable period of data loss, measured in time. It helps inform backup frequency and data protection planning.

RTO and RPO targets should reflect business priorities, application dependencies, data requirements, and available recovery capabilities. This overview does not set specific targets for any customer environment.

6. Recovery Testing and Validation

Review and test the recovery plan to confirm that its procedures meet recovery requirements. Testing can reveal gaps in backup coverage, restoration procedures, system dependencies, and service validation.

A testing approach may include:

1. Backup verification - Review protection status, coverage, and retention settings.
2. Restore testing - Restore selected data or workloads in an appropriate environment.
3. Service validation - Confirm that restored systems and applications function as expected within the scope of the test.
4. Results and improvements - Document findings, issues, and follow-up actions. Update procedures as the environment changes.

Set the scope and schedule recovery tests according to business requirements, recovery objectives, and the implemented configuration. Document the results of each test.

7. Planning and Scope

Infrastructure and recovery arrangements vary by environment. Workload selection, backup configuration, storage, access controls, recovery resources, and documented procedures all affect recovery capabilities.

Set recovery objectives with the people responsible for the business continuity and infrastructure. Review test results with them and update the recovery plan as needed. Each environment requires its own design and validation; recovery capabilities depend on the configuration and test results.

Discuss Your Requirements

NovaCore Systems can work with your organization to review infrastructure dependencies, backup needs, recovery priorities, and business continuity requirements for NovaCore Connect.

Contact NovaCore Systems to discuss your environment and recovery planning needs.